



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁷ : G06F 17/00</p>	A2	<p>(11) International Publication Number: WO 00/67143</p> <p>(43) International Publication Date: 9 November 2000 (09.11.00)</p>
<p>(21) International Application Number: PCT/NL00/00278</p> <p>(22) International Filing Date: 28 April 2000 (28.04.00)</p> <p>(30) Priority Data: 99201334.2 28 April 1999 (28.04.99) EP 09/543,602 5 April 2000 (05.04.00) US</p> <p>(71) Applicant (for all designated States except US): UNICATE B.V. [NL/NL]; Gooimeer 3-15, NL-1411 DC Naarden (NL).</p> <p>(72) Inventors; and (75) Inventors/Applicants (for US only): SIPMAN, Wilhelmus, Hendrikus, Maria [NL/NL]; Smidsweg 1A, NL-7433 BM Schalkhaar (NL). WARD, Scott, MacDonald [NL/NL]; Zuidlaan 31, NL-2111 GB Aerdenhout (NL).</p> <p>(74) Agent: H.V. MERTENS; Exter Polak & Charlois B.V., P.O. Box 3241, NL-2280 GE Rijswijk (NL).</p>		<p>(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>Without international search report and to be republished upon receipt of that report.</i></p>
<p>(54) Title: TRANSACTION METHOD AND SYSTEM FOR DATA NETWORKS, LIKE INTERNET</p>		
<p>(57) Abstract</p> <p>A method and a system for performing a transaction between at least one first party and at least one second party are disclosed. A data network connects data input/output terminals of the parties. In the data network a secure and trusted transaction server is provided, in which a profile of the parties is registered, having a party identifier identifying a particular party, and authentication data for authenticating the party and data sent by the party. The parties communicate with each other through the transaction server by means of various transaction messages, which are digitally signed using a table of random numbers and a hashing operation, wherein the table of random numbers is generated by reading a token.</p>		

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon	KR	Republic of Korea	PL	Poland		
CN	China			PT	Portugal		
CU	Cuba	KZ	Kazakhstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

TRANSACTION METHOD AND SYSTEM FOR DATA NETWORKS, LIKE INTERNET

FIELD OF THE INVENTION

5

The present invention relates to a transaction system for use with data networks, like intranets, extranets, and Internet. Transactions to be performed may include e-commerce, such as shopping and business-to-business transactions, electronic banking, protected
10 emailing, consulting and amending databases, brokerage, and the like. The invention also relates to the authentication of parties and the transactions exchanged. The invention further relates to the preparation of a confidential message. The invention still further relates to the generation of a digital signature as for use in the
15 transmission of secure information.

BACKGROUND OF THE INVENTION

When using data networks, like Internet, for transactions between
20 parties, that want to exchange information, that want to buy goods, enjoy services or receive information and other parties offering those goods, services or information, one of the problems observed is the lack of secure and at the same time simple transaction methods. Secure systems, such as SET, SSL, etcetera exist, but are
25 felt as being cumbersome to use, involving heavy message traffic, (complex) cryptographic procedures, and key management including key recovery.

SUMMARY OF THE INVENTION

30

An object of the invention is to provide a secure data network transaction system without the need for cryptography, whilst fulfilling demands for security, particularly privacy, authentication and irrefutability of the messages that constitute a
35 transaction.

The privacy requirements are that no information is disclosed to any party, unless needed to perform the basic objective, which within the scope of this invention comprises the execution of a transaction, with or without a payment that might result from the transaction.

The authentication requirements are to be able to verify the authenticity of transmitted data and the sender of those data. Within the scope of this invention these data, as well as an identification of the parties concerned, form part of transaction messages.

The basis of the invention is to use a secure and trusted computer environment, referred hereinafter as the transaction server. Parties wishing to use the services of the transaction server, are registered at the server with a so called profile. Such profile contains at least the data necessary to provide data integrity, data authentication, authentication of the parties, confidentiality of sensitive data (privacy) and irrefutability.

In such an environment, there will be two types of parties: a party that demands a service, a product, or information, further referred to as a "customer"; and a party that offers such services, products, or information, further referred to as a "supplier".

In case the transaction involves a payment, a third type of party may occur: one or more financial institutions that take care of the payment process, further referred to as a "financial institution". In the system according to the invention, the number of customers, suppliers and/or financial institutions may range from 1 to many. One or more of the objects of the invention are reached by a method for performing at least one transaction between at least one first party and at least one second party using at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party, the method comprising:

- (a) providing a transaction server in the at least one data network;
- (b) in the transaction server, registering a profile of the at least one first party and the at least one second party, each
- 5 profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the authentication data comprising a table of random data for verifying a digital signature;
- (c) the first party issuing at least one transaction message to the
- 10 second party;
- (d) in response to the transaction message, the second party issuing a digitally signed transaction confirmation message to the first party;
- (e) on the basis of the transaction confirmation message, the first
- 15 party issuing a digitally signed transaction approval message to the transaction server;
- (f) if required by the first or the second party, the transaction server verifying the authenticity of the first party and the second party, and the transaction data, in response to the transaction
- 20 approval message;
- (g) the transaction server issuing a verified transaction approval message to the second party, in case said authenticity verification is required only if the verification is positive, resulting in a verified transaction approval message; and
- 25 (h) fulfilment of the transaction.

An example of such a transaction is a customer to supplier transaction or a business to business transaction, where a customer or business demands a service, a product, or information.

30

The invention further discloses a method for performing at least one transaction between at least one first party and at least one second party using at least one data network for interconnecting data input/output devices of the at least one first party and the at

35 least one second party, the method comprising:

- (a) providing a transaction server in the at least one data network;

- (b) in the transaction server, registering a profile of the at least one first party and the at least one second party, each profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the authentication data comprising a table of random data for verifying a digital signature;
- (c) the first party issuing at least one transaction message to the transaction server;
- (d) in response to the transaction message, the transaction server verifying the authenticity of the first party, and the transaction data;
- (e) if the verification is positive, the transaction server issuing a verified transaction message to the second party; and
- (f) the second party and the first party performing the at least one transaction through the transaction server by means of digitally signed messages, the validity of which is verified by the transaction server.

Examples of such a method are brokerage or telebanking, where the first party is a customer, and the second party is a supplier of services.

Use of the invention for sending and retrieving electronic mail is obtained by a method for performing at least one transaction between at least one first party and at least one second party using at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party, the method comprising:

- (a) providing a transaction server in the at least one data network;
- (b) in the transaction server, registering a profile of the at least one first party and the at least one second party, each profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the authentication data comprising a table of random data for verifying a digital signature;

- (c) the first party issuing at least one digitally signed transaction message to the transaction server;
- (d) in response to the transaction message, the transaction server verifying the authenticity of the first party;
- 5 (e) if the verification is positive, the transaction server linking the transaction message to the profile of a second party;
- (f) if the second party connects to the transaction server, the transaction server verifying the authenticity of the second party; and
- 10 (g) if the verification is positive, the transaction server issuing the transaction message to the second party.

Here, the transaction message is an email.

- 15 The invention further discloses a method for performing at least one transaction between at least one first party and at least one second party using at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party, the method comprising:
- 20 (a) providing a transaction server in the at least one data network;
- (b) in the transaction server, registering a profile of the at least one first party, the profile comprising a party identifier identifying the party, and authentication data for authenticating
- 25 the party and data sent by the party, the profile further comprising operation identifiers each identifying an operation that is enabled for the party, and is meaningful only between the party and the transaction server;
- (c) the first party issuing at least one transaction message to the
- 30 transaction server;
- (d) in response to the transaction message, the transaction server verifying the authenticity of the first party, and the transaction data;
- (e) if the verification is positive, the transaction server issuing
- 35 a verified transaction message to the second party; and
- (f) the second party and the first party performing the at least one transaction through the transaction server.

Such a method is particularly suitable for a party desiring to gain access to a service provider anonymously. Yet the service provider can be sure that the party is entitled to the requested access.

5

Instead of using a table of random data for verifying a digital signature, the profile may comprise operation identifiers each identifying an operation which is enabled for the party, and is meaningful only between the party and the transaction server.

10

In the system according to the invention, the need for encryption is eliminated as there are no sensitive data to be exchanged between customer, supplier and transaction server. The sensitive data are replaced by covert coded data, which are significant only to the sender and receiver of the message, thus respecting the privacy.

15

The authentication problems are solved by non-cryptographic methods, hence avoiding the problems of key management and the computing power to perform cryptographic operations. Even, when cryptographic digital signatures are used, the authenticity can be more easily established, using the transaction server concept according to the invention.

20

Additionally, transaction irrefutability is achieved, since every step in the process can be monitored and verified.

25

If the transaction involves payments, the transaction server does not require any adaptations within the existing payment systems, as it uses transparently the network structures, which are in use today for the processing of electronic payment transactions. This is quite a cost saving factor, as changing anything in these systems is not a trivial operation. At the same time, the use of the transaction server opens new channels for making frequent payments of small amounts of money, as the costs of processing these payments is low.

30

35

FURTHER ASPECTS OF THE INVENTION

Having the secure and trusted transaction server, this server may offer other services, like controlled access to services, payment methods based upon pre-authorisation or electronic cash, loyalty schemes, etc.

- 5 Loyalty schemes can easily be implemented by adding bonus counters to the customer's profile. With the transaction system according to the invention it is possible to add opportunities for 1-1 marketing between various suppliers (like merchants, issuer banks and acquirer banks) and customers. The loyalty scheme is based upon a data file, added to the customer's profile, which can be accessed e.g. as an Internet HTML page or similar.

- Furthermore, provisions may be made to enable a user to access the facilities, offered through the transaction system, from another
15 device than his base device (i.e. the device which is standard configured for transactions according to the invention).

- The invention and its advantages will be more readily appreciated as the same becomes better understood by reference to the following
20 detailed description and considered in connection with the accompanying drawings in which like reference symbols designate like parts.

BRIEF DESCRIPTION OF THE FIGURES

- 25 FIG. 1 is a diagram of a transaction system according to the present invention.
FIG. 2 illustrates how a party applies for participation in the transaction system.
30 FIG. 3 illustrates the relation between the various functional entities.
FIG. 4 illustrates the steps in a sample transaction.
FIG. 5 illustrates how a party can obtain a temporary profile where a party uses a device not personalised for him.
35 FIG. 6 illustrates the generation of a digital signature used for verifying the authenticity of the data and the sender of those data.

FIG. 7 illustrates how a random structure can be used to generate a table of random numbers.

FIG. 8 illustrates steps in a sample transaction between parties.

FIG. 9 illustrates a transaction, involving a direct payment.

- 5 FIG. 10 illustrates a supplier controlled environment, e.g. for electronic banking or brokerage, using the transaction server concept.

FIG. 11 illustrates steps in exchanging marketing information between parties.

- 10 FIG. 12 illustrates steps in accessing a service provider anonymously.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

- 15 FIG. 1 is a diagram of a transaction system in accordance with the invention. Centrally there is a secure and trusted data processing system, hereinafter to be referred to as a transaction server 1, to which participating parties 2, 3 are connected through a data network 4, e.g. Internet. If the transaction involves a payment, the
20 transaction server 1 connects to one or more financial institutions 6, using the existing payment networks 5. The transaction server holds so-called profiles 7 and 8 for the participating parties, as explained below with reference to FIG. 2. "Users" of the transaction system are parties 2 ("Customer") that want to obtain goods,
25 services and/or information from other parties 3 ("Supplier"), who are suppliers of these goods, services and/or information. The parties 2, 3 are selectively coupled to the data network 4.

- Financial institutions 6 involved are Issuers (banks issuing payment cards to clients), Acquirers (banks serving the needs for suppliers
30 of goods, services and/or information), and Schemes (financial institutions managing payment cards, like VISA, Mastercard and the like).
- 35 FIG. 2 illustrates how a party 12, 13 will be registered to be able to participate in the transaction system. In Step A the party 12, 13 fills in an application form, containing his request to participate

in the transaction system, his identification and (if payment is included in his profile) a list of payment methods (which cards, debit or credit, etc.) he wants to use (if he is a payer/consumer 12) or a list of payment accepting methods (which accounts, etc.) he wants to use (if he is a supplier 13) and an authorisation to the transaction server 11 to verify his account/card data at the corresponding bank and receive additional information, required to create the party's profile. The application form then is submitted to the institution, operating the transaction server 11, on paper, by E-mail, by courier, or otherwise.

Next, Step B, the account/card information together with the identification of the applying party 12, 13 is sent to a Registration Authority 10 (R.A.), e.g. his bank relation(s) to verify the authenticity of the party 12, 13 and the information supplied with his application.

The request to participate in the transaction system may also directly be addressed to the Registration Authority 10 (the dashed line in FIG. 2).

If the Registration Authority 10 of the party 12, 13 verifies the party positively, i.e. party's identity and other information match, it sends an approval message (Step C) to the organisation operating the transaction server 11. Using the approval message content of Step C in the transaction server 11 a profile for the party will be built, Step D.

Each profile contains at least the party's identification and those other data, which are required to process the transactions as being used.

The profile further may contain data, relevant to a personalised token, which has been or will be issued to the party.

Although cryptography is not required for the invention, still the profile may contain cryptographic keys, to enhance the security of the communication between the transaction server and the party.

The profile may contain a random data string, which acts as a pseudonym for the party identified. The profile further may contain

a payment method list, indicating the various payment methods permitted for that party.

Each payment method in the profile may be identified by a random data string.

The profile may contain further data fields for other applications, e.g. electronic cash, loyalty programs, telebanking, stock
5 brokerage, etc.

Finally, in Step E, the organisation operating the transaction server 11, which may also be a supplier or a bank, ensures that the party receives a personalised package, required to interface with the transaction system offered, and to be used with the party's data
10 processing system to be coupled to the data networks. The content of this package (data, program and token) mirrors the profile, as registered in the transaction server. Parts of the package may be distributed to the party, using other channels, including electronic means, like electronic mail, or using other suppliers, e.g. a shop,
15 the Registration Authority, or the like.

In FIG. 3 various entities are indicated.

Parties 21, 23 that want to make use of the transaction system may use a token reader 22, 24. This token reader is used to read the
20 token, required for generating a digital signature of (selected parts of) message(s) in the transaction. Parties communicate through a data network 26, e.g. Internet. A secure and trusted transaction server 20 is also connected to the same data network, in order to receive messages from parties 21, 23. The transaction server 20
25 processes the transactions, after thorough verification of the validity of the transactions, using the party's profiles, as stored in the transaction server 20. If the transaction involves a payment, the payment process (authorisation and settlement) is handled through the payment network 25, using the procedures that apply for
30 such situations.

When the customer 2 in FIG. 1 wants to perform a transaction from another location than his base location (the location equipped with standard configured/personalized means for performing transactions
35 according to the invention), or otherwise is requested to authenticate himself, this can be achieved by downloading a temporary set of data and program, as depicted in step E in FIG. 2

at the not at base location. A not at base location could be a workstation at the office, a Cybercafe, a PDA (Personal Digital Assistant) with mobile phone function attached, or otherwise, provided that such a system offers access to the data network and is
5 equipped with a token read facility.

As soon as an authentication request is due and the not at base system detects an unknown token (i.e. a token, which is not registered with the token reader, data and program, as referred to
10 in step E of FIG. 2), the user is prompted to enter data, containing the address of the transaction server, his remote ID and, if required, his password. If the token possesses a memory, these data may be obtained from that memory. A message is built, containing the user data entered and provided with a hash and (token based)
15 signature, similar to the payment order as in (c) of FIG. 9, to be discussed below. The message is now transferred to the transaction server which, after verification of the correctness of the message received and the existence of a profile for that user, will send a temporary set of data and program to the not at base system. Now the
20 not at base system is able to prepare a transaction message, or to authenticate the user, and proceed as normal. Depending of the agreed conditions, the temporary set of data and program will be erased or maintained for a set period.

25 FIG. 4 depicts a sample flow for a typical transaction.

- (a) A first party 30 and a second party 31 negotiate a transaction. In an Internet environment the first party, e.g. a customer will through his browser visit a site of the second party (e.g. a supplier) and request for a transaction, e.g. purchase goods,
30 buy and sell stock, obtain information, or the like.
- (b) The second party may require some proof of identity of the first party. He therefore sends a "Who are You" message to the first party.
- (c) The first party adds his identity, as registered in his profile
35 33 at the transaction server 32 to the "Who are You" message and completes the message with a unique transaction number, a Hash total calculated over the previous data items, and his

digital signature. This message ("I am") is then transferred to the transaction server.

- (d) The transaction server verifies the message, received from the first party. If the message and the first party are verified positively, the server sends a message to the second party, confirming the identity of the first party and requesting the second party to identify himself.
- (e) The second party adds to the message, received from the server, his identity, as registered in his profile 34, a "form" (e.g. a HTML page in case of Internet) in which the first party can fill in the details of his transaction request, a unique transaction number, a Hash total calculated over the previous data items, and his digital signature.
- (f) Similar to step (d), the transaction server verifies the message received from the second party and his identity. If verified positively, the form is transferred to the first party.
- (g) The first party now fills in the form with the transaction details, as requested, adds a unique transaction number, a Hash total and his digital signature, and sends it to the server.
- (h) The server verifies the message and, if verified positively, transfers the filled in form to the second party.
- (i) The second party replies to the transaction details, as filled in in the form with a message, completed with a unique transaction number, a Hash total calculated over the previous data items, and his digital signature.
- (j) The server verifies the message received, and if verified positively, transfers the reply to the first party.
- Steps (g) to (j) may be repeated, if more transactions are to be performed in the same session.
- The verification of the messages as in (d), (f), (h) and (j) may be executed on the basis of a risk profile. If the risk profile does not demand immediate verification, the verification may be postponed until a request of either party is received to verify the messages, e.g. in case of a dispute about a certain transaction.
- The creation of the digital signature may be performed as described in FIG. 9 below.

FIG. 5 depicts a sample flow how a party 40 can obtain a temporary profile, if he uses another system than the one, which has been personalised according to step E in FIG. 2.

- 5 Where in FIG. 4 step (c) should start, the system detects a token, for which the system has not been personalised.

- (a) It therefore sends a request to the server 42 to receive a temporary profile. The message contains at least the server address and a user identification. These data are either collected from the first party's token, using a token reader 41 or entered manually. To enhance the security the message may be provided with a digital signature, generated in the same way as at the payment order. For further security the first party may have to include a Personal Identification Number (PIN) or any other personal identifier, e.g. a password or biometric quality.
- 10
15

- (b) After positive verification of the request for a temporary profile, using the party's profile 43, the server returns a message, containing a temporary personalised package, which is in essence the same as in step E of FIG. 2, but may contain certain usage restrictions, like validity period or services granted. The validity period may be one transaction, a limited number of transactions, or an agreed time period, whatever has been agreed at the time the profile has been set up (step D in FIG. 2).
- 20
25

- As an additional service, the server may log the full transaction details, to be collected by the first party at a later time, when he connects to the server from the system, which has initially been personalised for using the transaction method described.
- 30

POINTER METHOD

- With the pointer method, as depicted in FIG. 6, it is possible to generate an electronic signature over a given set of data.
- 35

Assume a table 46 of random numbers. The table 46 may be the read result of a token, e.g. a 3DAS® card. Assume the number of elements in the table 46 equals n . Further assume that each number has a value between 0 and 255.

- 5 Assume the defined length of the signature is m bytes, where m is smaller than n .

In the example, depicted in FIG. 6, n equals 35 and m equals 5. Then an electronic signature over a given set of data D can be calculated:

- 10 compress D , using a hashing technique and/or some other method resulting into d ;
 d has the property that it can be split into at least n digits, each representing a value between 1 and m ; preferably m is replaced by m' , where m' is the largest power of 2 smaller than m .
15 In the example d becomes the string: 1, 9, 20, 16, 30;
identify the elements in the table of random numbers with the values 1 to m . In the example the elements are numbered column by column, starting at the top;
the digital signature now is the string of values of the
20 elements taken from the random table, identified by the values in d . In the example the digital signature becomes the string:
128, 27, 5, 99, 38.

- FIG. 7 illustrates how a table of random numbers may be generated,
25 using a material with a random structure.

- Assume a token (e.g. a credit card), which is provided with a random two dimensional or three dimensional structure (e.g. a 3DAS® card). The token is inserted in a token reader 50. In the token reader 50 an image is taken from the random structure in the token, which is
30 in the case of a 3DAS® card an image as the sample image 51. In the image empty spaces are visible between the mapping of the random structure as blank areas. The areas are measured, and the n largest areas are selected (52). For each of the selected areas its Centre of Gravity (CoG) is calculated as a pair of coordinates (53). A
35 table 54 now is filled with the sizes (first column of the table) and the corresponding coordinates of the CoG (second and third

columns of the table). As the original material used is random, also the values in the table 54 are random.

Referring again to FIG. 1, the customer is indicated with 2 and the supplier with 3. The customer profile may contain, as earlier indicated, among others the account/card related data and data fields for other applications, e.g. electronic cash, loyalty programs, electronic banking, stock brokerage, etc. To enable 1-1 marketing a further data file is added. It should be noted, that all the information, stored in the customer profile is present with the customer's agreement, as he did sign up for the transaction solution described. Upon given criteria, any of the parties 2, 3 and 6 may leave a message in the data file, destined for one of the other parties. This message is stored in the format, applicable for the network solution chosen, through which the customer communicates with the transaction server. In case of Internet this will be an HTML page or the like.

As soon as the destination party connects to the transaction server and the party's authenticity has been established, he will be prompted by the transaction server that a message is present for him. The party may neglect the prompt or decide to read the message. The message itself may link to other messages, stored elsewhere in the data network (e.g. Internet).

E.g., if an acquirer wants to make an offer to the customer, the message may contain links to the acquirer's website, containing further information. As an example, an acquirer may offer extra bonus miles if the customer selects Mastercard as payment method for paying an international flight. The message then could be an HTML page: 'Dear customer, you may earn extra bonus miles if you pay your international flight, using your Mastercard. If you are interested, visit our website at www.Acquirer.com'. If the customer is interested, he just clicks the website's reference and can access all the relevant data on how to obtain the extra bonus miles and the conditions.

The criteria, used to add a message to the customer profile, may refer to general attributes, belonging to the profile, e.g. which payment methods are enabled for that customer, or refer to specific attributes, e.g. the current transaction, his collected bonus etc.

5

If a first party wishes to send a message to a second party based upon a given selection criterion, applicable to such second party, the first party sends the message together with the selection criterion to the transaction server. The transaction server now
10 selects all second parties, that match the criterion and adds to their profiles a data file, containing the message concerned, or if such data file already exists, adds the message to that data file. The criterion may include a validity time, i.e. a time within which this criterion should be applied. In that case the transaction
15 server will monitor changes in the second party's profile. If such a change might result in that the second party meets the criterion, the message is added to his profile as described above. As an example, an issuer may offer a special financing arrangement to any customer buying a car during a given month. The criterion is a
20 customer buying a car. The validity time is the given month. As soon as the transaction server detects a transaction, in which a customer is buying a car (or might be expected to do so, based upon the supplier's profile, i.e. the supplier is a car seller), the transaction server adds the message to the customer's profile and
25 prompts the customer that there is a message for him.

When applying this method the privacy of the customer is guaranteed: no information is disclosed to (in the example) the issuer, unless the customer decides to contact the issuer and apply for the special
30 financing arrangement.

If no direct payment is involved between a first and a second party, FIG. 8 shows how the transaction will be protected, whereby the authentication of both parties, the transaction messages and the
35 irrefutability of the transaction can be guaranteed, using the same mechanisms as described hereafter with reference to FIG. 9. The first party is the one, requesting a service. The first party may be

a consumer, but also a professional (as in business to business electronic commerce, B2B). The second party is the supplier of the requested services.

In step (50) the first party visits a site of the second party and indicates his desire to perform a certain kind of transaction. The second party sends a signed request for log-in to the first party (51), whereby his signature is generated similarly to the invoice message as in step (b) of FIG. 9 to be described hereafter.

The first party processes the log-in request (52) similar to preparing a payment order, as in step (c) of FIG. 9 and transmits the message to a secure transaction server.

The server verifies the message from step (52), using the profiles of both parties. If verification is positive, the server passes the log-in data to second party (53).

The second party checks the authorisation of the first party to perform the requested transaction and returns a signed application form (54) to the server. The application form is a data file (e.g. an HTML page) the first party can use to enter the transaction data. The server verifies the validity of the application form and

transfers it to the first party (55).

The first party fills in the application form and signs it similar to the payment order message as in step (c) of FIG. 9. The form is then transmitted (56) to the server.

After verification by the server (57) the application form is passed to the second party, to be further processed.

Steps (54) to (57) may be repeated, depending on the context of the transaction.

Authenticity of the parties, the transaction and its irrefutability are thus guaranteed by the secure transaction server.

30

FIG. 9 depicts a sample flow for a typical transaction involving a payment.

(a) A first and a second party negotiate a purchase. In an Internet environment the first party, e.g. a consumer will through his browser visit a site of the second party (e.g. a merchant) and pursue a normal electronic shopping process by picking goods and storing them in a so-called shopping basket. When he has

35

completed the shopping process, he sends a buying order to the second party.

- (b) If the second party accepts the order, he will prepare an invoice message and transmit this to the first party.

5 The invoice message contains: an identification of the second party, a content of the sale, an amount due, a payment accepting method, a unique transaction number, a Hash total (HashM) calculated over the previous data items, and a digital signature of the second party, calculated over HashM, as exemplified below.

10 The identification of the second party may be replaced by his pseudonym, as registered at the transaction server, to enhance privacy as his true identity now is covert, without the need for cryptography.

15 The payment accepting method may be replaced by the random selected key, pointing to the required payment accepting method, as registered in the transaction server, to enhance privacy as his payment accepting method data now are covert, without the need for cryptography.

20 The digital signature may be generated using a token. The digital signature may be generated using the pointer method, as elucidated below. The token used in this case may be a 3DAS® object, such as a card, with an optically scannable three-dimensional pattern of randomly overlying fibres, as disclosed in U.S. Patent Nos. 5,354,097 and 5,719,939, and Dutch Patent No. 1,000,330, which documents are incorporated herein by reference. The card can be read with an appropriate reading device. This eliminates the need for cryptography.

30 If a 3DAS® card is used as token, any jitter in the reading of the mark of the card may be used to make the transaction number unique and guarantees at the same time, that the token has been read and processed.

- 35 (c) After receiving the invoice, the first party prepares a payment message and transmits this to the transaction server. This message contains: an identification of the first party, a copy

of the invoice message, a payment method, a unique transaction number, a Hash total (HashC) calculated over the previous data items, and a digital signature of the first party, calculated over HashC, as exemplified below.

5 The content of the sale may be deleted from the copy of the invoice message, enhancing privacy by not transmitting this information.

The HashC may be deleted from the payment message.

10 The identification of the first party may be replaced by his pseudonym, as registered at the transaction server, to enhance privacy as his true identity now is covert, without the need for cryptography.

15 The payment method may be replaced by a random selected key, pointing to the required payment method, as registered in the transaction server, to enhance privacy as his payment method data now are covert, without the need for cryptography.

The digital signature may be generated using a token.

20 The digital signature may be generated using the pointer method as elucidated below. The token used in this case may be a card like a 3DAS® card. This eliminates the need for cryptography. If a 3DAS® card is used as token, the jitter in the reading of the card may be used to make the transaction number unique and guarantees at the same time, that the token has been read and processed.

25 The digital signature also may include a personal identification, such as a Personal Identification Number (PIN) as is generally used when one wants to withdraw money through an Automated Teller Machine (ATM), a personal identification code or character string, a biometric feature, or any other feature which is strictly personal.

30 (d) After receiving the payment message, the transaction server starts verifying the message received. Depending on first party's payment method and second party's payment accepting method the authenticity of both parties are verified by the transaction server itself or by a financial institution
35 concerned.

If 3DAS® cards are used as token, the transaction numbers, generated by either party will prove that an actual read has been performed, reducing the chance for counterfeit attacks, such as replay.

- 5 (e) Using the information in the first and second party's profiles the transaction server now builds an authorisation request message and/or settlement messages as agreed with the financial institution concerned. In the example of FIG. 9 an authorisation request message is build and transmitted to an
- 10 acquirer bank (a merchant's bank as indicated by his payment accepting method).
- (f) If the authorisation for the payment is granted, the financial institution concerned (in the example of FIG. 9 the acquirer bank) will prepare for settlement of the payment transaction.
- 15 (g) The financial institution concerned will inform the transaction server whether the payment is authorised.
- (h) Finally the transaction server informs both parties about the result of the authorisation.
- 20 These messages may contain a random number, which then is used to modify the party's pseudonym and the keys, identifying the payment methods. This will reduce the possibilities for possible attackers to replay a transaction or to act as impostor.

- 25 In FIG. 10 a configuration for telebanking or electronic banking is described. In this case there is only one party, the client of a bank. The party is via an open network, e.g. Internet, connected to the secure transaction server similar as the situation described in FIG. 1. Similarly the client's bank is connected to the server via
- 30 a closed network.

- (60) When the client wants to perform one or more telebanking transactions, he sends a log-in request to the server, signed and protected in the same way as the payment order message (as (c) in FIG. 4).
- 35 (61) The server verifies the authenticity of the client and checks if a relation with the specified bank exists and/or the client is

allowed to perform a specific transaction. If so, the log-in request is (via the secure closed network) transmitted to the client's bank. The bank will respond with an Application Form (62), being a data file, where the client can enter the data concerning the transaction requested. This data file may be in case of Internet an HTML page. (63) The server signs the Application Form and transfers it to the client.

The client completes the Application Form with the transaction data required (64), applying the same protection and signature mechanisms, as used in the payment order as in (c) in FIG. 4 and sends it to the server.

After inspection of the signed Application Form, the server passes it to the client's bank (65).

If required, steps (62) till (65) are repeated, until all transactions are transmitted.

Authenticity of the party, the transaction(s) and the irrefutability are thus guaranteed by the secure transaction server.

Referring to FIG. 11, parties may exchange marketing information using the profiles (items 7, 8 in FIG. 1), where a party S is the sender and a party R is the receiver of the information. The identity of party R is hidden to party S, unless party R decides to directly contact party S to further investigate the information transmitted to party R. According to a step 70, the party S wants to submit a message to one or more parties R, based upon predefined criteria. For this purpose, party S therefore sets a criteria scheme. This scheme indicates on what basis the one or more parties R have to be addressed, and the time duration of the message to be submitted to the one or more parties R (i.e. the time period during which the message is valid and may be sent). Furthermore, party S defines the message contents. This message may contain a reference to a special offer and/or references to (in case of Internet) a website of party S.

According to a step 71, party S then sends the criteria scheme and the message to the server. According to a step 72, the server analyses the criteria scheme and selects those one or more parties R, that meet the criteria scheme. If a duration is specified, the

server monitors all transaction occurrences of the one or more parties R, to find out if they will fit into the criteria scheme, due to a change in their continuously updated profile. If a transaction occurrence of a party R is found, meeting the criteria

5 scheme, the message is added to his profile together with a "flag", which is an indicator indicating that the criteria scheme is met. According to a step 73, as soon as an occurrence of a party R contacts the server, e.g. by issuing a payment order, and the "flag" is set, the server informs this party R that a message is present.

10 The party R may decide to read the message or to ignore it. If the party R reads the message, he may react to the contents of the message or neglect it.

A party may want to access a certain service provider, without

15 disclosing his true identity. The service provider, in turn, may or may not want to be sure that the party is entitled to the requested access. FIG. 12 shows how a party can get anonymous access to a service provider.

In step (80) the party sends a signed request to the secure

20 transaction server to access a certain service provider. The server verifies the identity of the party and, if required, its right to access a requested service, using the party's profile. If the party is verified positively, the server transmits an access request message to the service provider, using a pseudonym for the party.

25 The service provider now knows that the access request is legitimate, since the request originates from the transaction server and starts a dialogue (82) with the (anonymous) party through the server, which transfers the messages to the party (83). At the choice of the party, the party might disclose his true identity to

30 the service provider during this dialogue.

EXAMPLES OF THE USE OF THE INVENTION

A consumer wants to buy a book via Internet at an Internet

35 bookseller. He selects the book wanted from the inventory of the bookseller and places an order. The bookseller now prepares a digitally signed invoice message. In this message the bookseller's

identity is hidden by the reference to his profile at the transaction server, as is his payment accepting method. As the invoice message arrives at the computer of the consumer, he is prompted with a "pay" request. The consumer now inserts his token in the token reader and selects his method of payment. Next, the program in his computer prepares a payment message to the transaction server. In this message only the data from the invoice message, which are relevant for the payment process, are copied. The identity and selected method of payment are hidden by referring to his profile at the transaction server. The payment message finally is provided with the consumer's digital signature.

The transaction server now can process the payment request in basically three ways.

1. If the payment method selected is a cash payment, the account in the consumer's profile is debited for the amount due, while the account in the bookseller's profile is credited for the same amount. (Note: the cash method is more likely to be used for buying services, like searching a database, or information, like an audio file of the latest top hit).
2. If the payment method selected is a debit or credit transaction, and the transaction server is entitled by the financial institutions concerned to verify the authenticity of the consumer and the bookseller, then a simple authorisation request message or even a settlement request message will be sent to the corresponding financial institution.
3. If the payment method selected is a debit or credit transaction, and the transaction server is not entitled by the financial institutions concerned to verify the authenticity of the consumer and the bookseller, then an authorisation request message is sent to the corresponding financial institution, which then has to verify the authenticity of the consumer and bookseller, and inform the transaction server about the result of the authorisation.

Finally, the transaction server informs the consumer and retailer about the result of the payment order and optionally provides them with a random number, to modify the pointers to their profile data.

- 5 The privacy of the payment transaction in the above examples is guaranteed simply by not transmitting privacy sensitive information, but only references to data, already available at the transaction server.

- 10 The authentication of the payment transaction and its initiators is done by verifying the digital signatures.

Protection against hacking can be offered by changing the pointer values after each payment transaction, at fixed time intervals or after a given number of transactions.

- 15 The software required for implementing the method according to the invention, or one of the features thereof, is recorded on a computer readable medium, such as a floppy disk, a hard disk, a magnetic tape or other suitable media, to make a data processing system execute procedures in accordance with the method or one of the features
20 thereof.

CLAIMS

1. A method for performing at least one transaction between at least one first party and at least one second party using at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party, the method comprising:
- (a) providing a transaction server in the at least one data network;
 - (b) in the transaction server, registering a profile of the at least one first party and the at least one second party, each profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the authentication data comprising a table of random data for verifying a digital signature;
 - (c) the first party issuing at least one transaction message to the second party;
 - (d) in response to the transaction message, the second party issuing a digitally signed transaction confirmation message to the first party;
 - (e) on the basis of the transaction confirmation message, the first party issuing a digitally signed transaction approval message to the transaction server;
 - (f) if required by the first or the second party, the transaction server verifying the authenticity of the first party and the second party, and the transaction data, in response to the transaction approval message;
 - (g) the transaction server issuing a transaction approval message to the second party, in case said authenticity verification is required only if the verification is positive, resulting in a verified transaction approval message; and
 - (h) fulfilment of the transaction.
2. The method of claim 1, wherein the profile further comprises operation identifiers each identifying an operation which is enabled for the party, and is meaningful only between the party and the transaction server.

3. A method for performing at least one transaction between at least one first party and at least one second party using at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party, the method comprising:
- (a) providing a transaction server in the at least one data network;
 - (b) in the transaction server, registering a profile of the at least one first party and the at least one second party, each profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the profile further comprising operation identifiers each identifying an operation which is enabled for the party, and is meaningful only between the party and the transaction server;
 - (c) the first party issuing at least one transaction message to the second party;
 - (d) in response to the transaction message, the second party issuing a digitally signed transaction confirmation message to the first party;
 - (e) on the basis of the transaction confirmation message, the first party issuing a digitally signed transaction approval message to the transaction server;
 - (f) in response to the transaction approval message, the transaction server verifying the authenticity of the first party and the second party, and the transaction data;
 - (g) if the verification is positive, the transaction server issuing a verified transaction approval message to the second party; and
 - (h) fulfilment of the transaction.
4. The method of claim 1 or 3, wherein the profiles further comprise payment method identifiers identifying authorized methods of payment, the method further comprising before fulfilment of the transaction:
- (g1) the transaction server requesting an authorisation to at least one financial institution for authorising a payment from the first party to the second party;

(g2) in response to the authorisation request, the financial institution informing the transaction server whether the payment is authorised; and

(g3) the transaction server informing the first party and the second party about the result of the authorisation.

5. The method of claim 4, wherein step (b) comprises:

(b1) each party providing payment information to the transaction server about each method of payment to be used in conjunction with the party;

(b2) the transaction server verifying the payment information with at least one financial institution;

(b3) the at least one financial institution providing the transaction server with transaction data necessary for the method of payment to be performed;

(b4) the profiles further comprising the transaction data for each method of payment.

6. The method of claim 1 or 3, wherein the parties each establish an account held by the transaction server, the method further comprising before fulfilment of the transaction:

(a) for settling a payment from the first party to the second party, the transaction server debiting the account of the first party, and crediting the account of the second party; and

(b) the transaction server informing the first party and the second party about the result of the payment.

7. A method for performing at least one transaction between at least one first party and at least one second party using at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party, the method comprising:

(a) providing a transaction server in the at least one data network;

(b) in the transaction server, registering a profile of the at least one first party and the at least one second party, each profile comprising a party identifier identifying the party, and

authentication data for authenticating the party and data sent by the party, the authentication data comprising a table of random data for verifying a digital signature;

- (c) the first party issuing at least one transaction message to the transaction server;
- (d) in response to the transaction message, the transaction server verifying the authenticity of the first party, and the transaction data;
- (e) if the verification is positive, the transaction server issuing a verified transaction message to the second party; and
- (f) the second party and the first party performing the at least one transaction through the transaction server by means of digitally signed messages, the validity of which is verified by the transaction server.
8. The method of claim 7, wherein the profile further comprises operation identifiers each identifying an operation which is enabled for the party, and is meaningful only between the party and the transaction server.
9. A method for performing at least one transaction between at least one first party and at least one second party using at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party, the method comprising:
- (a) providing a transaction server in the at least one data network;
- (b) in the transaction server, registering a profile of the at least one first party and the at least one second party, each profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the profile further comprising operation identifiers each identifying an operation that is enabled for the party, and is meaningful only between the party and the transaction server;
- (c) the first party issuing at least one transaction message to the transaction server;

(d) in response to the transaction message, the transaction server verifying the authenticity of the first party, and the transaction data;

(e) if the verification is positive, the transaction server issuing a verified transaction message to the second party; and

(f) the second party and the first party performing the at least one transaction through the transaction server by means of digitally signed messages, the validity of which is verified by the transaction server.

10

10. A method for performing at least one transaction between at least one first party and at least one second party using at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party, the

15 method comprising:

(a) providing a transaction server in the at least one data network;

(b) in the transaction server, registering a profile of the at least one first party, the profile comprising a party identifier

20 identifying the party, and authentication data for authenticating the party and data sent by the party, the profile further comprising operation identifiers each identifying an operation that is enabled for the party, and is meaningful only between the party and the transaction server;

25 (c) the first party issuing at least one transaction message to the transaction server;

(d) in response to the transaction message, the transaction server verifying the authenticity of the first party, and the transaction data;

30 (e) if the verification is positive, the transaction server issuing a verified transaction message to the second party; and

(f) the second party and the first party performing the at least one transaction through the transaction server.

35 11. A method for performing at least one transaction between at least one first party and at least one second party using at least one data network for interconnecting data input/output devices of

the at least one first party and the at least one second party, the method comprising:

- (a) providing a transaction server in the at least one data network;
- 5 (b) in the transaction server, registering a profile of the at least one first party and the at least one second party, each profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the authentication data comprising a table of random data
- 10 for verifying a digital signature;
- (c) the first party issuing at least one digitally signed transaction message to the transaction server;
- (d) in response to the transaction message, the transaction server verifying the authenticity of the first party;
- 15 (e) if the verification is positive, the transaction server linking the transaction message to the profile of a second party;
- (f) if the second party connects to the transaction server, the transaction server verifying the authenticity of the second party; and
- 20 (g) if the verification is positive, the transaction server issuing the transaction message to the second party.

12. The method of claim 11, wherein, if the verification of the authenticity of the second party is positive, the transaction server

25 issues a transaction confirmation message to the first party.

13. The method of claim 1, 3, 7, 9, 10 or 11, wherein the at least one first party and the at least one second party are provided with personalized means for assembling electronic messages, including

30 transaction data associated thereto.

14. The method of claim 13, wherein for each party the means for assembling electronic messages are personalized by:

- (a) the party issuing a personalization message to the transaction
- 35 server;
- (b) on the basis of the personalization message, the transaction server verifying the authenticity of the party; and

(c) if the verification is positive, the transaction server issuing a set of data and program to the party.

15. The method of claim 14, wherein the personalization message
5 comprises:

- an address of the transaction server;
- the party identifier; and
- an optional password code.

10 16. The method of any of claims 1-4 and 7-11, wherein the identifiers are randomly selected.

17. The method of any of claims 1-4 and 7-11, wherein before the last step the transaction server modifies at least one of the
15 identifiers, and subsequently informs each party concerned about the at least one modified identifier.

18. The method of claim 1, 3, 7, 9, 10 or 11, wherein at least one of the first party identifier and the second party identifier
20 comprises a random data string.

19. The method of claim 1, 3, 7, 9, 10 or 11, wherein at least one message from a member of the group comprising the at least one first party and the at least one second party to any of the other members
25 of said group is stored at the transaction server, and transmitted to said any of the other members of said group upon connection of said any of the other members of said group with the transaction server.

20. The method of claim 19, wherein the message is associated with at least one criterion, the method further comprising:

- (a) selecting any member of said group matching said at least one criterion, and
- (b) issuing said message to said selected member of said group.

35 21. The method of claim 19, wherein the message is associated with a message validity time period, the method further comprising:

- (a) selecting any member of said group connecting to the transaction server within the message validity time period, and
- (b) issuing said message to said selected member of said group.

5 22. The method of claim 19, wherein the group comprises a financial institution.

23. The method of claim 1, 3, 7, 9, 10 or 11, wherein at least one of the messages is signed by:

- 10 (a) subjecting message data to a hashing operation, resulting in a hashing code;
- (b) providing a digital signature on the basis of the hashing code; and
- (c) adding the digital signature to the message.

15

24. The method of claim 23, wherein the digital signature includes a personal identification.

25. The method of claim 23, wherein the digital signature is

20 generated by:

- (a) providing a table of n random numbers, each having a predetermined position in the table;
- (b) dividing the hashing code into m digits, each representing a value between 1 and n, where m is smaller than n; and

25 (c) assembling a string of the random numbers of which the position in the table is indicated by the digits.

26. The method of claim 25, wherein the table of random numbers is generated by reading a token.

30

27. The method of claim 25 or 26, wherein the table of random numbers is generated by optically scanning geometrical configurations of a randomly shaped twodimensional or threedimensional mark.

35

28. A method for signing a message containing data, comprising:

- (a) subjecting the message data to a hashing operation resulting in a hashing code;
 - (b) providing a digital signature on the basis of the hashing code; and
 - 5 (c) adding the digital signature to the message.
29. The method of claim 28, wherein the digital signature is generated by:
- 10 (a) providing a table of n random numbers, each having a predetermined position in the table;
 - (b) dividing the hashing code into m digits, each representing a value between 1 and m, where m is smaller than n; and
 - (c) assembling a string of the random numbers of which the position in the table is indicated by the digits.
- 15 30. A method for generating a digital signature over a message, comprising:
- (a) providing a table of n random numbers, each having a predetermined position in the table;
 - 20 (b) splitting the message into m digits, each representing a value between 1 and n, where m is smaller than n; and
 - (c) assembling a string of the random numbers of which the position in the table is indicated by the digits.
- 25 31. A data processing system for performing at least one transaction between at least one first party and at least one second party, the system comprising:
- 30 (a) at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party;
 - (b) a transaction server in the at least one data network;
 - (c) means for registering a profile of the at least one first party and the at least one second party in the transaction server, each profile comprising a party identifier identifying the party, and
 - 35 authentication data for authenticating the party and data sent by the party, the authentication data comprising a table of random data for verifying a digital signature;

(d) means for assembling electronic messages by the first party and the second party;

(e) means for issuing at least one transaction message by the first party to the second party;

- 5 (f) means for issuing a digitally signed transaction confirmation message by the second party to the first party in response to the transaction message;

(g) means for issuing a digitally signed transaction approval message by the first party to the transaction server on the basis of
10 the transaction confirmation message;

(h) means for verifying the authenticity of the first party and the second party, and the transaction data by the transaction server in response to the transaction approval message;

- (i) means for issuing a verified transaction approval message by
15 the transaction server to the second party, if the verification is positive.

32. The system of claim 31, wherein the profile further comprises operation identifiers each identifying an operation which is enabled
20 for the party, and is meaningful only between the party and the transaction server.

33. A data processing system for performing at least one transaction between at least one first party and at least one second
25 party, the system comprising:

(a) at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party;

(b) a transaction server in the at least one data network;

- 30 (c) means for registering a profile of the at least one first party and the at least one second party in the transaction server, each profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the profile further comprising operation identifiers each
35 identifying an operation which is enabled for the party, and is meaningful only between the party and the transaction server;

(d) means for assembling electronic messages by the first party and the second party;

(e) means for issuing at least one transaction message by the first party to the second party;

5 (f) means for issuing a digitally signed transaction confirmation message by the second party to the first party in response to the transaction message;

(g) means for issuing a digitally signed transaction approval message by the first party to the transaction server on the basis of
10 the transaction confirmation message;

(h) means for verifying the authenticity of the first party and the second party, and the transaction data by the transaction server in response to the transaction approval message;

(i) means for issuing a verified transaction approval message by
15 the transaction server to the second party, if the verification is positive.

34. The system of claim 31 or 33, wherein the profiles further comprise payment method identifiers identifying authorized methods
20 of payment, the system further comprising:

(a) means for requesting an authorisation by the transaction server to at least one financial institution for authorising a payment from the first party to the second party;

(b) means for informing the transaction server by the financial
25 institution whether the payment is authorised, in response to the authorisation request; and

(c) means for informing the first party and the second party by the transaction server about the result of the authorisation.

30 35. The system of claim 34, wherein the profile registering means comprises:

(b1) means for providing payment information by each party to the transaction server about each method of payment to be used in conjunction with the party;

35 (b2) means for verifying the payment information by the transaction server with at least one financial institution;

(b3) means for providing the transaction server by the at least one financial institution with transaction data necessary for the method of payment to be performed, wherein the profiles further comprise the transaction data for each method of payment.

5

36. The system of claim 31 or 33, further comprising:

(a) means for establishing an account held by the transaction server by each party;

(b) means for debiting the account of the first party, and crediting the account of the second party by the transaction server, for settling a payment from the first party to the second party; and
10 (c) means for informing the first party and the second party by the transaction server about the result of the payment.

15 37. A data processing system for performing at least one transaction between at least one first party and at least one second party, the system comprising:

(a) at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second
20 party;

(b) a transaction server in the at least one data network;

(c) means for registering a profile of the at least one first party and the at least one second party in the transaction server, each profile comprising a party identifier identifying the party, and
25 authentication data for authenticating the party and data sent by the party, the authentication data comprising a table of random data for verifying a digital signature;

(d) means for assembling electronic messages by the first party and the second party;

30 (e) means for issuing at least one transaction message by the first party to the transaction server;

(f) means for verifying the authenticity of the first party, and the transaction data by the transaction server in response to the transaction message;

35 (g) means for issuing a verified transaction message by the transaction server to the second party, if the verification is positive;

(h) means for performing the at least one transaction by the second party and the first party through the transaction server by means of digitally signed messages; and

(i) means for verifying the validity of the digitally signed messages by the transaction server.

38. The system of claim 37, wherein the profile further comprises operation identifiers each identifying an operation which is enabled for the party, and is meaningful only between the party and the transaction server.

39. A data processing system for performing at least one transaction between at least one first party and at least one second party, the system comprising:

(a) at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party;

(b) a transaction server in the at least one data network;

(c) means for registering a profile of the at least one first party and the at least one second party in the transaction server, each profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the profile further comprising operation identifiers each identifying an operation that is enabled for the party, and is meaningful only between the party and the transaction server;

(d) means for assembling electronic messages by the first party and the second party;

(e) means for issuing at least one transaction message by the first party to the transaction server;

(f) means for verifying the authenticity of the first party, and the transaction data by the transaction server in response to the transaction message;

(g) means for issuing a verified transaction message by the transaction server to the second party, if the verification is positive;

(h) means for performing the at least one transaction by the second party and the first party through the transaction server by means of digitally signed messages; and

(i) means for verifying the validity of the digitally signed
5 messages by the transaction server.

40. A data processing system for performing at least one transaction between at least one first party and at least one second party, the system comprising:

10 (a) at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party;

(b) a transaction server in the at least one data network;

(c) means for registering a profile of the at least one first party
15 in the transaction server, the profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the profile further comprising operation identifiers each identifying an operation that is enabled for the party, and is meaningful only between the party and the
20 transaction server;

(d) means for assembling electronic messages by the first party and the second party;

(e) means for issuing at least one transaction message by the first party to the transaction server;

25 (f) means for verifying the authenticity of the first party, and the transaction data by the transaction server in response to the transaction message;

(g) means for issuing a verified transaction message by the transaction server to the second party, if the verification is

30 positive; and

(h) means for performing the at least one transaction by the second party and the first party through the transaction server.

41. A data processing system for performing at least one
35 transaction between at least one first party and at least one second party, the system comprising:

- (a) at least one data network for interconnecting data input/output devices of the at least one first party and the at least one second party;
- (b) a transaction server in the at least one data network;
- 5 (c) means for registering a profile of the at least one first party and the at least one second party in the transaction server, each profile comprising a party identifier identifying the party, and authentication data for authenticating the party and data sent by the party, the authentication data comprising a table of random data
- 10 for verifying a digital signature;
- (d) means for assembling electronic messages by the first party and the second party;
- (e) means for issuing at least one digitally signed transaction message by the first party to the transaction server;
- 15 (f) means for verifying the authenticity of the first party by the transaction server in response to the transaction message;
- (g) means for linking the transaction message by the transaction server to the profile of a second party, if the verification is positive;
- 20 (h) means for verifying the authenticity of the second party by the transaction server, if the second party connects to the transaction server; and
- (i) means for issuing the transaction message by the transaction server to the second party, if the verification is positive.
- 25
42. The system of claim 41, further comprising means for issuing a transaction confirmation message by the transaction server to the first party, if the verification of the authenticity of the second party is positive.
- 30
43. The system of any of claims 31-34 and 37-41, comprising means for randomly selecting the identifiers.
44. The system of any of claims 31-34 and 37-41, further
- 35 comprising:
- (a) means for modifying at least one of the identifiers by the transaction server; and

(b) means for informing each party concerned about the at least one modified identifier.

45. The system of claim 31, 33, 37, 39, 40 or 41, wherein at least one of the first party identifier and the second party identifier comprises a random data string.

46. The system of claim 31, 33, 37, 39, 40 or 41, wherein the transaction server comprises a server message section for storing at least one message from a member of the group consisting of the at least one first party and the at least one second party to any of the other members of said group.

47. The system of claim 46, wherein the public data network has a network message section stored on it, and the message contains a link to said network message section.

48. The system of claim 46, wherein the message is associated with at least one criterion, the system further comprising:

(a) means for selecting any member of said group matching said at least one criterion; and

(b) means for issuing said message to said selected member of said group.

49. The system of claim 46, wherein the message is associated with a message validity time period, the system further comprising:

(a) means for selecting any member of said group connecting to the transaction server within the message validity time period; and

(b) means for issuing said message to said selected member of said group.

50. The system of claim 31, 33, 37, 39, 40 or 41, wherein the means for assembling electronic messages comprise:

(a) means for issuing a personalization message by the first party and the second party to the transaction server;

(b) means for verifying the authenticity of the first party and the second party by the transaction server on the basis of the personalization message from the first party and the second party;

(c) means for issuing a set of data and program by the transaction server to the first party and the second party.

51. The system of claim 31, 33, 37, 39, 40 or 41, comprising means for signing at least one message by:

(a) subjecting message data to a hashing operation, resulting in a hashing code;

(b) providing a digital signature on the basis of the hashing code; and

(c) adding the digital signature to the message.

52. The system of claim 51, comprising means for generating the digital signature by:

(a) providing a table of n random numbers, each having a predetermined position in the table;

(b) dividing the hashing code into m digits, each representing a value between 1 and n , where m is smaller than n ; and

(c) assembling a string of the random numbers of which the position in the table is indicated by the digits.

53. The system of claim 52, comprising a token and a token reader for generating the table of random numbers.

54. The system of claim 53, wherein the token is an object provided with an optically scannable randomly shaped twodimensional of threedimensional mark.

55. A data processing system for signing an message containing data, comprising:

(a) means for subjecting the message data to a hashing operation resulting in a hashing code;

(b) means for providing a digital signature on the basis of the hashing code; and

(c) means for adding the digital signature to the message.

56. The system of claim 55, comprising means for generating the digital signature having:
- (a) means for providing a table of n random numbers, each having a predetermined position in the table;
 - (b) means for dividing the hashing code into m digits, each representing a value between 1 and m , where m is smaller than n ; and
 - (c) means for assembling a string of the random numbers of which the position in the table is indicated by the digits.
57. A data processing system for generating the digital signature, comprising:
- (a) means for providing a table of n random numbers, each having a predetermined position in the table;
 - (b) means for dividing the hashing code into m digits, each representing a value between 1 and m , where m is smaller than n ; and
 - (c) means for assembling a string of the random numbers of which the position in the table is indicated by the digits.
58. A computer program product comprising at least one computer readable medium, having thereon computer program code means, when said program is loaded, to make a data processing system execute procedure according to claim 1, 3, 7, 9, 10 or 11.
59. A computer program element comprising computer program code means to make a data processing system execute procedure according to claim 1, 3, 7, 9, 10 or 11.
60. The computer program element of claim 59, embodied on a computer readable medium.
61. A computer readable medium having a program recorded thereon, where the program is to make a data processing system execute procedure according to claim 1, 3, 7, 9, 10 or 11.

FIG. 1

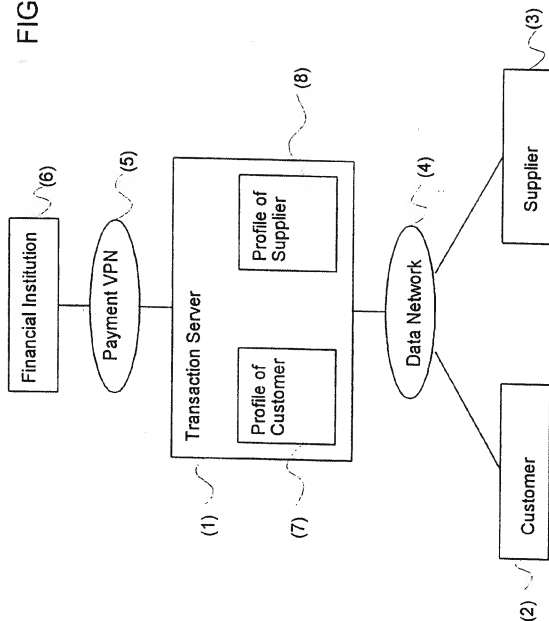


FIG. 2

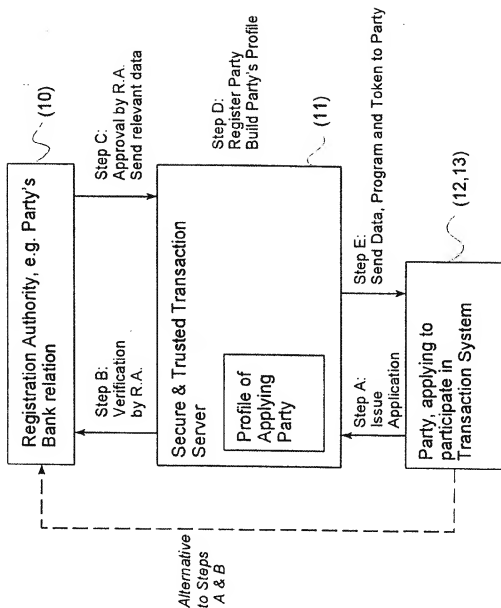
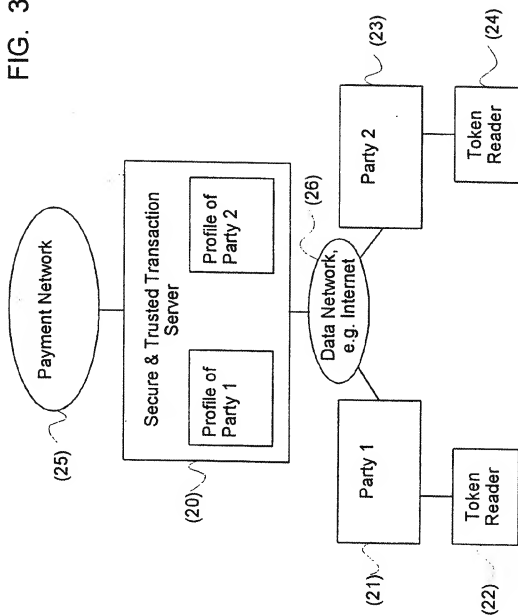


FIG. 3



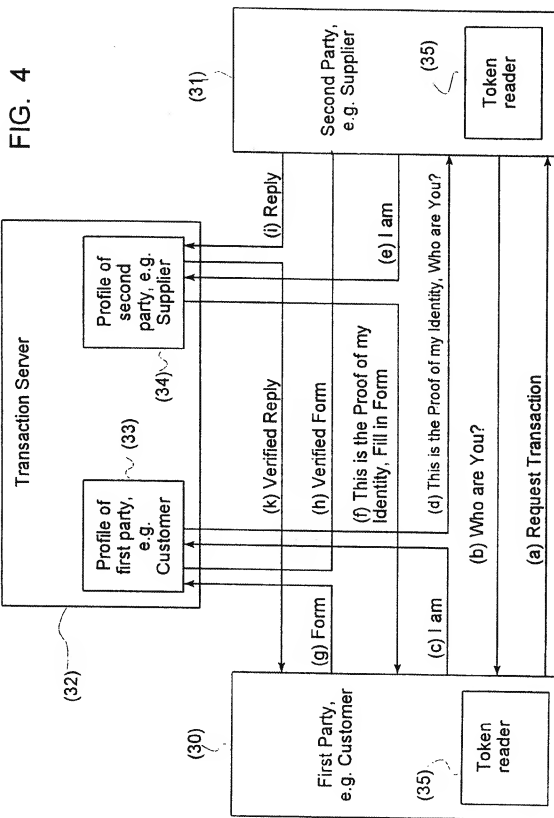


FIG. 5

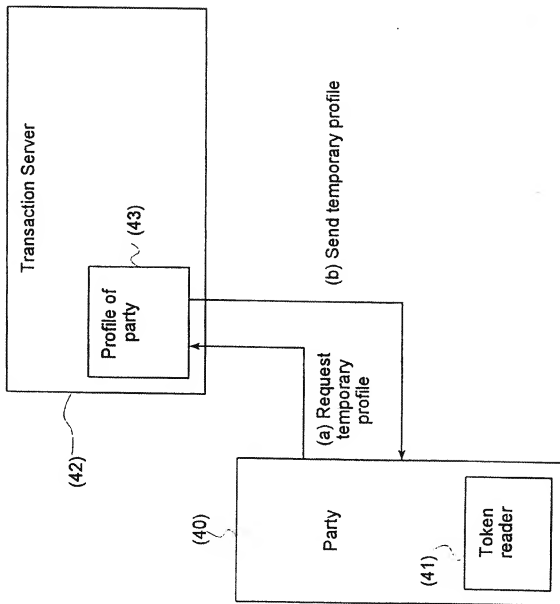
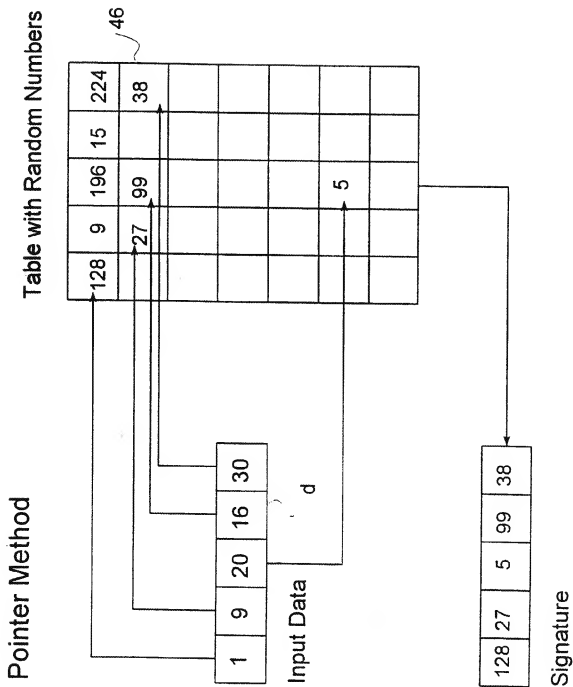


FIG. 6



7/12

FIG. 7

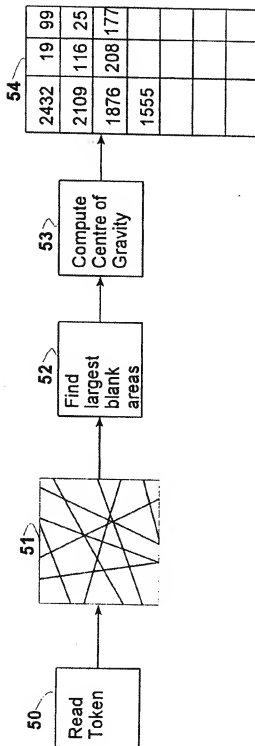
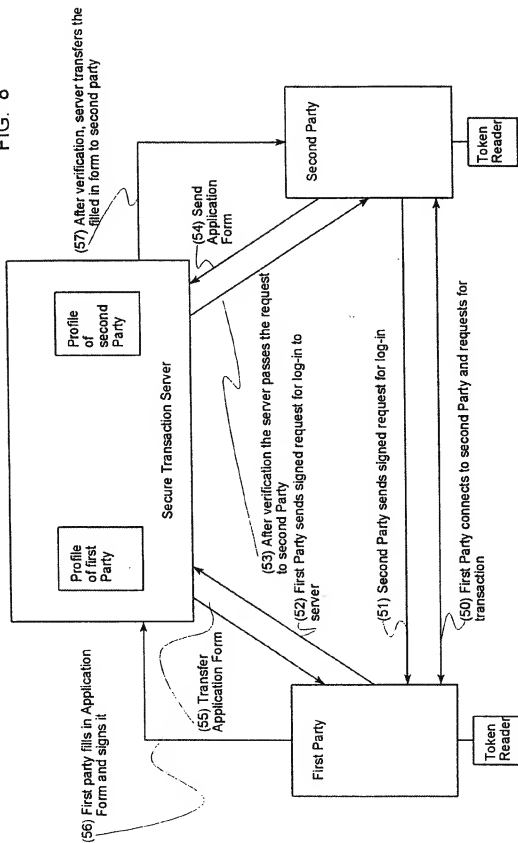


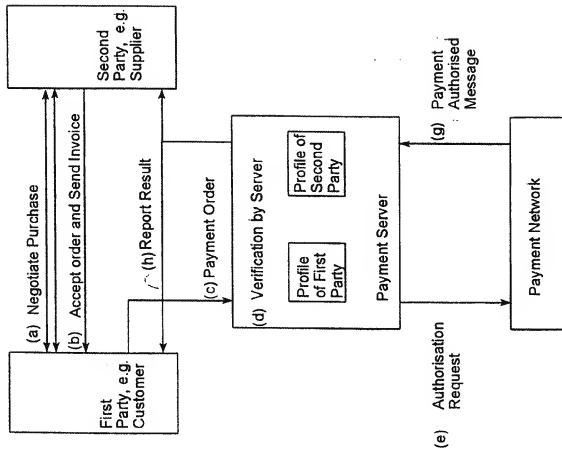
FIG. 8



9/12

Sample Transaction Flow

FIG. 9



10/12

FIG. 10

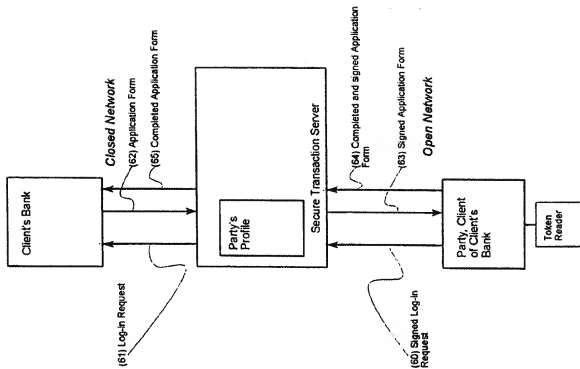
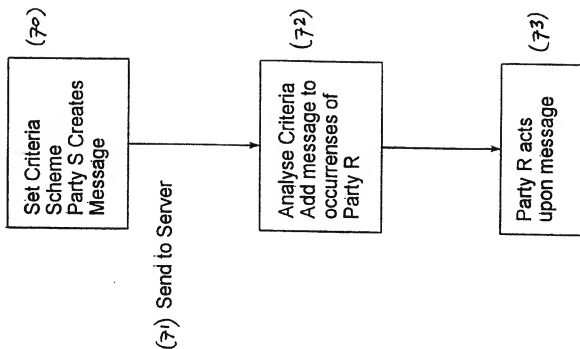
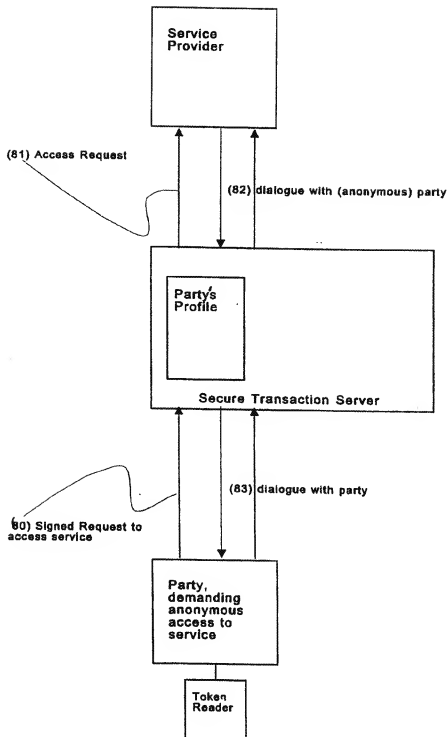


FIG. 11



12/12

FIG. 12



(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
13 September 2001 (13.09.2001)

PCT

(10) International Publication Number
WO 01/67201 A2

- (51) International Patent Classification: G06F (74) Agents: DANIELSON, Mark, J. et al.; Pillsbury Winthrop LLP, 1100 New York Avenue, N.W., Washington, DC 20005 (US).
- (21) International Application Number: PCT/IB01/00549
- (22) International Filing Date: 27 February 2001 (27.02.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Date: 60/187,927 8 March 2000 (08.03.2000) US
- (71) Applicant (for all designated States except US): AURORA WIRELESS TECHNOLOGIES, Ltd. [CN/CN]; 18F, No. 1 Pao Sheng Road, Yang-Ho City, Taipei (TW).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MY, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

(72) Inventors; and

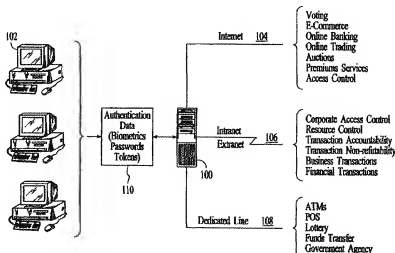
(75) Inventors/Applicants (for US only): CAMACHO, Luz, Maria [US/US]; 107 Tate Court, Orlando, FL 32828 (US).
 PIRKEY, Roger, D. [US/US]; 165 Broadmoor Road, Lake Mary, FL 32746 (US).
 HANKINSON, Michael, L. [US/US]; 2186 Mt. Evans Boulevard, Pine, CO 80470 (US).

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR REDUCING ON-LINE FRAUD USING PERSONAL DIGITAL IDENTIFICATION



(57) Abstract: A distributed Personal Digital Identification (PDI) system and architecture rapidly verifies individuals using biometric data or other tokens prior to approving a transaction and/or granting access to an on-line services and other network services. The architecture that includes a server that has access to template data required to authenticate individuals, and the processing capacity to route authenticated requests to the appropriate downstream entity (Internet Service Provider, Credit Card Company, etc.). The server is connected to requesting users by various network methods to form a client/server architecture. The server and clients each contain discrete subsystems, which provide various levels of authentication services to users of the system.

WO 01/67201 A2

METHOD AND APPARATUS FOR REDUCING ON-LINE FRAUD USING PERSONAL DIGITAL IDENTIFICATION

CROSS-REFERENCE TO RELATED APPLICATION

5 The present application is based on, and claims priority from, U.S. Appln. No. 60/187,927, filed March 8, 2000 and entitled "Method and Apparatus for Reducing On-Line Fraud Using Personal Digital Identification," commonly owned by the assignee of the present application, the contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

10 1. Field of the Invention

The present invention relates to data communications and E-commerce, and more particularly, to a method and apparatus for detecting and reducing fraudulent use of Business-to-Consumer (B2C), Business-to-Business (B2B) and other transaction services using Personal Digital Identification (PDI) techniques.

15 2. Description of the Related Art

With the growing use of the Internet and the concurrent increase of E-commerce and other Business-to-Consumer (B2C) transactions, purchases of goods and services that are conducted without an individual present to show identification will also increase. Access to on-line accounts is also granted without the presence of an individual to confirm or authenticate the accessing user.

20 One B2C transaction problem of concern is credit card fraud. Hackers, scam artists, and criminals can always find a weak link in conventional authentication methods. This is because, although many measures have been developed to protect the card-issuing banks and consumers against fraud, they provide only illusory protection – what is authenticated is information that is known or possessed, not the individual. Accordingly, after the industry stops one leak, another leak is
25 discovered and exploited.

Another B2C problem of growing concern is employee abuse of company resources, as access by employees to the Internet using company equipment is readily possible in most companies. Although not all employees abuse Internet service, the cumulative use of all employees can result in much time and resources being taken away from an employer.

30 Relatedly, supervision of a child's on-line activities is a concern for parents. Although there are many "parental control" software products available on the market, most reside directly on the end-user's PC and can be turned off at any time by either the minor or the parent and in some cases be circumvented by other software applications.

35 Another growing concern is subscription/account fraud. The exchange of account information among individuals is decreasing the revenues received by Internet Service Providers

(ISPs). In addition to lost revenue on subscriptions that are not paid for comes the requirement for additional capacity to support authorized and unauthorized users accessing ISP services.

In addition to lost revenue from unauthorized "subscribers," ISPs have other concerns. Many ISPs host web pages. One potential problem is if an intruder gains access to the host, the intruder may be able to change information on the host's web page, thus possibly subjecting the ISP to further liability. Moreover, an intruder could use a public web site as an entry point into a company's internal files and gain access to confidential information such as competitively sensitive business information or information about the company's clients and/or employees that could be protected by privacy laws. This could be particularly serious for an ISP that is also a cable company, which maintains extensive customer data. A related problem, referred to as a "Trojan Horse," occurs when an intruder enters an ISP web site with the intention of gaining unauthorized access to other computer systems by concealing his/her true identity by use of the web site. Once again, potential ISP liability arises if the intruder launches his or her attack from the ISP's web site. Counteractive efforts that an ISP can undertake range from common-sense precautions to reporting suspicious activity to the FBI. Some of the more conventional methods include: posting a log-in banner that warns unauthorized users that they may be subject to monitoring; using audit trails within the computer network; keystroke level monitoring; caller identification; establishing internal passwords and changing them frequently; installing anti-virus software on every PC; installing "firewall" software to limit access; making back-ups of any damaged or altered files; maintaining old back-ups to demonstrate the status of the original; designating one person to secure potential evidence of fraudulent activity; establishing procedures to secure tape back-ups and print-outs.

In addition to B2C transactions, Business-to-Business (B2B) transactions encounter many of the same difficulties in authenticating the validity of activities committed by an individual. Although corporate and individual Digital Certificates and passwords/Personal Identification Numbers (PINs) are currently deployed, they can be shared and exploited if in the wrong hands.

All the conventional methods for reducing fraud have drawbacks and limitations. Primarily, firewalls and other logins and passwords do not protect against unauthorized access where the thief already knows account information, passwords or possesses digital credentials. Similarly, post-hoc fraud detection procedures can only be effective if the unauthorized user can be found and prosecuted.

Accordingly, there remains a need for a method and apparatus for proactively reducing transaction-based fraud where the requesting individual is not known, or physically present, to provide identification.

SUMMARY OF THE INVENTION

Generally, the present invention provides a method and apparatus for authenticating transactions conducted by an individual or agent by comparing biometric data and/or profiles to known templates previously provided to the system in a certifiable environment. If transaction

authentication cannot be achieved, business rules of the apparatus are used to determine successive action.

In accordance with one aspect of the invention, in order to reduce or prevent unauthorized access to finances or other resources, the invention detects and controls both merchant and consumer transactions through the use of apparatus profiling and biometric credential comparisons. A dynamic profile is created and/or updated for each consumer/merchant using the invention, by means of adaptive learning techniques. The apparatus algorithms use transaction data vectors such as purchase patterns, method of payment, location of purchases and purchaser, and various other elements to create profile. Historical profiles and the current transaction are used to determine the method of authentication. System rules dictate conditions which must be met such as time of day, day of week, login location, or other established criteria, in order to authenticate/grant access to services. Depending upon pre-established business rules and the determined need for transaction authentication, biometric comparisons, digital code matching, a combination thereof, or other methods are deployed.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and advantages of the present invention, along with the best mode for practicing it, will become apparent to those skilled in the art after considering the following detailed specification, together with the accompanying drawings wherein:

FIG. 1 is a block diagram illustrating an overview implementation of the present invention;

FIG. 2 is a block diagram further illustrating an exemplary implementation of the present invention in accordance with a preferred embodiment;

FIG. 3 is a high-level flowchart illustrating an example method implemented by the PDI system in accordance with one embodiment of the present invention;

FIGS. 4A – 4B further illustrate an example of the Filter Manager Process;

FIGS. 5A – 5B further illustrate an example of the Identity Manager Process;

FIG. 6 provides a flowchart illustrating an example of a Registration Process;

FIGS. 7A – 7C further illustrate an example of the Transaction Rules Manager Process;

FIGS. 8A – 8C further illustrate an example of the User Profile Manager Process;

FIGS. 9A – 9C further illustrate an example of the Authentication Manager Process; and

FIG. 10 is a flowchart illustrating an example of the Client Software Process.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates an overview implementation of the present invention, in which PDI system 100 interacts with persons using clients 102 who seek access to resources through such routes as the Internet 104, intranet/extranet environments 106 and dedicated or leased lines 108. In accordance with an aspect of the invention, in some cases system 100 requires such persons to provide unique

personal identification information 110 such as fingerprints or tokens before permitting access to services, or approving a transaction via the services, thus protecting consumer and provider alike from fraud or misuse by unauthorized individuals.

The access routes 104, 106 and 108 shown in FIG. 1 are intended to be illustrative rather than limiting. Those skilled in the art will understand that not all these types of accesses need be included and that other types of access routes may be added while remaining within the concept of the invention. Further, although other services are capable of being provided and/or controlled by the present invention, as shown in FIG. 1, Internet 104 accessed services can include, for example, on-line voting, e-commerce, on-line banking, on-line trading, auctions, premium services and access control. Intranet/extranet environment 106 accessed services can include, for example, corporate access control, resource control, transaction accountability, transaction non-refutability, business transactions, financial transactions. Dedicated or leased line 108 accessed services can include, for example, automated teller machines (ATMs), point-of-sale (POS) terminals, lottery terminals, funds transfer terminals and government agency terminals. Generally, the principles of the present invention can be extended to other types of services and access routes in which identification authentication is desirable, as will be understood by those skilled in the art.

As will be described in more detail below, whereas conventional methods use post-hoc artificial intelligence or tracking procedures to determine when an account is potentially associated with fraudulent or abnormal behavior, if at all, the PDI system 100 of the present invention uses a combination of fraudulent behavior detection and identification verification measures to preemptively authenticate a purchase from, or access to, a service. For example, purchases over the Internet made using credit cards issued by banks may require PDI authentication all of the time due to the inability to verify users with mere account information. Alternatively, the PDI system 100 can generate a list of known purchase points (web sites) associated with a consumer, and when those sites are used in successive transactions, the consumer is not prompted to enter a PDI, because that activity is part of the consumer's current profile. In contrast, if the consumer initiates a purchase transaction at a site that is not part of the consumer's profile, the consumer will be prompted to enter the appropriate PDI authentication as a means of ensuring and verifying that the credit card belongs to the holder.

PDI system 100 maintains business rules (also known as constraints) in addition to the consumer's own PDI Profile. To meet security requirements of the specific domain, the PDI system administrator configures these business rules, as that term is used herein, based upon company (e.g. a card-issuing bank, an ISP or a company Intranet) needs. For example, business rules can include lists of sites that are marked as always requiring authentication regardless of historical profile, which sites have been identified as having been associated with fraud in the past. Conversely, business rules can determine which sites never require authentication, or only constrain authentication by specific rule sets, such as sites that are considered secure and typically not associated with suspicious activity.

PDI system 100 further provides pre-emptive security for card-issuing banks and other network services. For example, if an account is being used fraudulently, the individual committing fraud may have access to the account holder's name, address, account number and other information that is typically required to allow access to the account. Another case is that of "Account" information shared among multiple individuals. For example, an individual who subscribes to a service that requires a login and password may share the login and password data among several individuals who now use the service fraudulently, with only one billable account.

As will be described in more detail below, PDI system 100 preferably includes a facility/server which provides PDI services and methods in accordance with the invention that protect consumers and service providers against unauthorized usage, and in particular, transactions over open networks. The PDI system 100 utilizes a database that stores and maintains unique identifying information, which identifying information constructs user and organizational profiles. Conventional information can also be stored, such as contact information, credit card numbers, transaction data, billing information, and related historical profile vectors. It should be understood that the PDI system of the invention may further include means to collect and process transaction information, and to build user profiles, company profiles, and default profiles based upon presented data.

The PDI system 100 is ordinarily located at a remote location relative to the clients 102, and can provide a centralized source of authentication for users that operate the clients 102 to seek access to resources of services through 104, 106 and 108. Alternatively, the system can reside upon company premises or be centralized to provide many establishments the PDI system in a service bureau manner. Although PDI system 100 is shown separately from the service providers accessed through Internet 104, intranet/extranet 106 and dedicated lines 108 for clarity of the invention, it should be understood that the installed location of the present invention is highly configurable due to its distributed design. For example, the PDI System 100 can reside directly at a site such as an electronic storefront; it can be located at an independent location such as a service bureau facility to process transactions from multiple locations; and/or can reside directly at the site whose service is being requested.

FIG. 2 is a block diagram illustrating an exemplary implementation of the present invention. Such an implementation will demonstrate the use of the PDI System 100 in an online retail environment. Those skilled in the art will be able to understand how to extend the principles of the invention to other types of environments after being taught by the foregoing example.

As shown in FIG. 2, the PDI System 100 includes a digital computer(s) acting as a server 204 that communicates with several subsystems: Filter Manager 208, Identity Manager 210, Transaction Rules Manager 212, User Profile Manager 214, Authentication Manager 216, and Administrative Services Manager 218, which subsystems can be implemented as software processes executing on one or more processors. . The digital computer(s) acting as a server 204 further communicate(s) with a

Data Storage Subsystem 220 that facilitates access to persistent PDI System 100 data by using functional procedure calls and requests to local or remote file system or data base management system (DBMS) processes and threads executing on one or more processors to access the data from one or more mechanical and/or solid state storage device(s). The various components of PDI system 100 can be interconnected by a network such as a LAN or WAN and communicate via protocols such as TCP. The PDI System 100 communicates with a client system 102, an electronic storefront 202, and a credit payment service 206 by way of data communications networks such as the Internet 104, intranet/extranet 106 and/or dedicated line 108. The exemplary implementation described in detail below will assume that the network components are connected via the Internet.

FIG. 2 further illustrates an example of a client 102 that can be used in the PDI system architecture of the present invention. As further shown in FIG. 2, the client system 102 is comprised of a digital computer 102a, a biometrics collection device 102b, an industry-standard web browser 102c, and PDI client software 102d.

Clients 102 will be described in detail herein with reference to the appropriate hardware and software needed to interact with server 204 for submitting user identification data to the PDI system 100 for authentication services and transactions. However, it should be apparent that clients 102 can include other conventional functionality that is not necessary for the present invention and therefore will not be described so as not to obscure the invention.

Digital computer 102a is preferably a PC or other type of computer that includes a data communications access device, such as a modem or other network interface, which allows the consumer to access the Internet. It should be understood that many alternatives to digital computer 102a are possible, and can include all computing devices that are, or can be used to communicate and conduct electronic-commerce and other access transactions over communications networks, with such computing devices including but not limited to servers, workstations, laptops, palm and handheld computers.

As will be described in more detail below, PDI client software 102d can be implemented as a plug-in application to industry-standard browser 102c, such as Internet Explorer or Netscape Communicator. In an example of the invention where fingerprints are used as the authenticating biometric data, biometrics collection device 102b and PDI client software 102d incorporate commercial fingerprint sensing devices and application program interfaces provided by vendors such as American Biometrics Corporation, Veridicom, etc., in order to format such collected data for communication with the PDI System 100.

The electronic storefront 202, in this example, is an Internet-based merchant site such as Amazon.com. The client system 102 accesses, and requests the purchase of goods or services from, electronic storefront 202 by means of industry-standard web browser 102c. The specific electronic storefront 202 generates the needed purchase forms, which in turn are filled out by the consumer and

submitted for processing by the electronic storefront 202. Once the form data has been submitted by the consumer, the electronic storefront 202 forwards the purchase request to the PDI System 100 for authentication determination and further processing. This process will be described in further detail below.

- 5 Communications between the client 102, the electronic storefront 202, the PDI web-enabled server 204, and the credit payment service 206 can be performed using standard Hypertext Transfer Protocol (HTTP) as implemented by industry standard web browsers and servers. Further communication protocols such as Common Gateway Interface (CGI) may be used to transfer HTML form data between system components. In general, the PDI system preferably uses known and
- 10 accepted protocol standards deployed within the World Wide Web such as Java Script and/or other client-side web-based APIs and programs, and server-side processes and APIs (e.g., C/C++, CGI, PHP, and other server-side APIs, or combination thereof).

- The PDI system 100 as further illustrated in FIG. 2 generally operates as follows. The PDI web-enabled server 204 accepts the purchase request from authorized electronic storefront sites. The
- 15 request is first processed to ensure that business-filtering rules are applied to the transaction by way of the Filter Manager 208. This filtering process quickly identifies those transactions that warrant further authentication, or which may be immediately rejected by the system. After the request is evaluated, the transaction is processed by the Identity Manager 210. The Identity Manager ensures that the required information is available to the PDI system 100 to properly identify the consumer and
- 20 ensure that registration information is available. After the Identity Manager 210 retrieves the consumer context, the Transaction Rules Manager 212 then processes the request. For example, the Transaction Rules Manager 212 processes the request against company level (i.e. business) rules to determine if authentication is required and, if so, what type should be requested of the consumer. After this determination, the User Profile Manager 214 evaluates the current request against historical
- 25 profile information associated with the consumer, and processes the request accordingly. When the User Profile Manager 214 completes the request evaluation, the resultant data is forwarded to the Authentication Manager 216 which, if required, initiates a dialog with the client 102, and collects and evaluates the authentication data against stored templates. If the authentication data is properly collected and authenticated, the request is forwarded to the credit payment service 206 for approval of
- 30 credits and debits. If the request is not properly authenticated, the requestor and the electronic storefront 202 are notified, and the purchase transaction does not complete, from a PDI system 100 perspective. The consumer must re-submit the transaction request again, if permitted to do so.

- Administrative Services Manager 218 permits system administrators to manage the PDI System 100 including, for example, to (1) manage attributes associated with PDI System 100 system
- 35 administration and PDI System 100 Subscriber/Consumer accounts; (2) generate change requests and problem reports; (3) access on-line PDI System 100 documentation; (4) generate reports detailing

with various aspects of the PDI System 100; (5) perform certain operations and maintenance (O&M) activities to ensure the health of the PDI System 100; and (6) create, modify, and delete Rule sets which affect PDI System 100 processing. With the exception of administration of Rule Sets, the above administration functions are generic in that they apply to almost all systems from a system administration standpoint. Generally, Rule Sets control the acceptance or denial of, or authentication method applied to, transactions passing through the PDI System 100.

In one example of the invention, there are eight broad Rule categories where associated business and other rules can be created, modified or deleted using the Rules functionality of the Administrative Manager 218. These eight Rule categories are: (1) Behavior, for threshold-based relationships; (2) Boolean, for simple logic (e.g., ship-to-address != bill-address); (3) Global, for processes and methods to be applied to all transactions; (4) Identity, for specific consumer-based activities; (5) Network, for specific network element-based activities; (6) Profiles, for aggregated transaction content-based activities; (7) Purchases, for single transaction content-based activities; and, (8) Transactions, for aggregated transaction externals-based activities.

The Global Rule category is the most controlling of the various Rule categories since its constraints affect each and every transaction processed by the PDI System 100. Only one of the following seven rules should be active at any given time: (1) No Global Constraints (PDI_AUTH_NONE), indicating that no constraints should be globally applied to each and every transaction. This is the default selection, and allows downstream rules processing to potentially determine the fate of a transaction; (2) Allow All Transactions (PDI_AUTH_ALLOW), indicating that each and every transaction is allowed to flow through the system without challenge. This effectively turns off the PDI System 100 Rule and Authentication logic; (3) Deny All Transactions (PDI_AUTH_DENY), indicating that each and every transaction should be denied without challenge. This effectively blocks all transactions from ever being sent to the Credit Payment Service 206; (4) Always Use Best Available (PDI_AUTH_BEST), indicating that for each and every transaction, the best method available on the Client 102a should be used, depending upon availability of the Biometric Collection Device 102b; (5) Always Use Biometrics (PDI_AUTH_FP), indicating that for each and every transaction, a biometric sample should be used to authenticate the requesting individual; (6) Always Use Digital Code (PDI_AUTH_DC), indicating that for each and every transaction, a matching Digital Code from the requesting individual is required; (7) Always Use Biometrics and Digital Code (PDI_AUTH_FP_DC), indicating that both a Digital Code and a biometric sample from the requesting individual is required.

The Network Rule category provides for the creation of Rules based on the network elements associated with a given transaction. Generally, such rules are in a format such as "If <domain> equals/does not equal <value>, then <authentication>," where <domain> can be, for example, Merchant Domain, Merchant Address, Merchant Name, Client Domain, Client Address and <value>

can be any User defined value, including wildcards, and <authentication> can be any authentication rule, such as PDI_AUTH_ALLOW, PDI_AUTH_DC, PDI_AUTH_BEST, PDI_AUTH_FP, PDI_AUTH_FP_DC, PDI_AUTH_DENY.

5 The Profiles Rule category provides for the creation of Rules based on data aggregates associated with both the current and historical activity of the transaction's requesting individual. Generally, such rules are in a format such as "If <domain> exceeds <quantity> within <time quantity>, then <authentication>," where <domain> can be, for example, Total Amount, Number of Transactions, Number of E-sites Visited, Number of ISP Login Sites, Number of Cards Used, Number of Authentication Failures, Number of Unique Ship-to-Addresses, Number of Unique Contact
10 Addresses, Number of Unique Billing Addresses, <quantity> can be any user specified numeric value, and <time quantity> can be any user specified time quantity.

The Purchases Rule category provides for the creation of Rules based on certain purchase related data elements of a given transaction. Such rules can be in a format such as "If <domain> equals/not equals/greater than/less than <value>, then <authentication>," where <domain> can be, for
15 example, Purchase Amount, Card Type, Expiration Date, Card Number, Bill-to-Country, Ship-to-Country and <value> can be a Domain specific user input or select list value.

The Transactions Rule category provides for the creation of Rules based on the network elements of a given transaction and a user defined time period. Generally, such rules can be in a format such as "If <domain> equals/not equals/greater than/less than/between/not between <time
20 period> of <value>, then <authentication>," where <domain> can be, for example, Any Activity, E-Commerce, Certificate Authority, Point-of-Sale, Internet Service Provider, <time period> can be Time of Day (TOD), Day of Week (DOW), Absolute Date (AD), TOD + AD, TOD + DOW, and <value> can be any domain-specific select list value.

The created business and other rules as described above, and as will be described in more
25 detail below, thus provide the authentication requirements used as a data resource of, or input data into, at least the Transaction Rules Manager 212, the User Profile Manager 214, and the Authentication Manager 216.

It should be noted that certain or all of the above-described rule administration functionality can be made available to users as well as system administrators via clients 102. For example, in
30 addition to a company establishing its own business rules, an individual can establish personal business rules, such as personal spending limits on a per-transaction or cumulative basis over a specified time interval in an online retail environment. Limits can also be placed on subordinate accounts to authenticate, restrict and control authorized users of system services as determined by the master account. For example, a parent or employer can create sub-accounts for each child and/or
35 employee and require authentication methods based on spending limits, access control, location, and

other profile constraints that limits and controls activities of the associated sub-account. Other vertical services can leverage the profiling capabilities of the apparatus as well.

The credit payment service 206, as used in this example, receives the credit authorization requests from the PDI system 100 upon successful transaction processing and/or authentication, if required. Credit payment service 206 can be implemented by a service such as, for example, CyberCash, which is responsible for authorizing credit card purchases, and if approved, transferring the appropriate credits/debits to/from the consumer and electronic storefront 202 accounts.

FIG. 3 provides a high-level transaction flow diagram that illustrates the use of a PDI system 100 of the present invention. In this example, communication with all system components is through the Internet 104. A consumer using client 102a and web browser 102c accesses a desired electronic storefront 202 and submits a purchase transaction request (block S302). The electronic storefront 202 accepts the consumer's transaction request for processing (block S304). The electronic storefront 202 redirects all or a subset of the consumer's transaction request data to the PDI system 100 for authentication determination and further processing (block S306). Redirection can be by means of a Uniform Resource Locator (URL) specification by the electronic storefront, or other accepted manner of specifying the global address of documents and other resources on the World Wide Web.

If the PDI system 100 determines in block S308 that user authentication is not required, the PDI system 100 invokes the specified payment service (block S316), and the transaction request is forwarded and processed by the credit payment service 206. If however, authentication is required, a dialog is initiated with the client web browser 102c (block S310). The consumer submits the requested authentication information using the web browser 102c and/or a combination of the web browser 102c, biometrics hardware collection device 102b, and PDI client software 102d depending upon the authentication requested. Upon completion of the authentication data collection, the client browser 102c submits this information directly to the PDI System 100 (block S312).

If the PDI System 100 verifies the collected information from the client 102a (determined in block S314), the transaction request is forwarded (block S316) to the credit payment service 206, which authorizes the credit card purchase on behalf of the consumer and electronic storefront 202. The resulting approval or disapproval is returned to the electronic storefront (block S320).

If the PDI System 100 rejects the authentication data, depending upon the business rules of the system (block S318), blocks S310 through S314 may be repeated for a configured number of times. If the PDI System 100 determines that blocks S310 through S314 are not to be repeated, the PDI System 100 returns a "reject" return result to the electronic storefront 202 (block S320).

The functionalities of the various subsystems of the example PDI system 100 illustrated in FIG. 2, as well as the various data structures from storage subsystem 220 that they use, will now be described in more detail. It should be noted that the ordering, selection and division of functionalities

performed by the various subsystems are not limited to the examples given below, and that those skilled in the art will recognize that many alternatives are possible.

FIG. 4A outlines the components that comprise, or are accessed by, the Filter Manager 208. In one example, this subsystem can be implemented by a CGI program that acts as the primary redirection URL when an electronic purchase transaction is sent through the PDI web-enabled server 204. As shown in FIG. 4A, Filter Manager 208 accesses several configuration/parameter files from data storage subsystem 220 during processing. As will be described in more detail below, these files 402 establish the business rules of the PDI system 100, and determine which (and how) transactions will be processed by PDI. In addition, template HTML files 404 may be used to construct error messages back to the Client browser 102c as necessary. Although not shown in FIG. 4A, it should be understood that data storage 220 further includes a session data table to handle data storage for tracking and maintaining the current state of individual transaction sessions. The data table maintains transaction time, client IP address etc. and allows the PDI system 100 to monitor and allow transactions only from the same client by using stored components to validate the authenticity of the information received. Further, although shown separately for clarity of the invention, it should be noted that files 402 and 404 can be implemented as part of data storage subsystem 220.

FIG. 4B is a diagram illustrating an example of the processing flow for Filter Manager 208. In one example of the invention, electronic storefronts 202 redirect payment authorization requests to PDI system 100 instead of the usual payment gateway services used to process credit card transactions. In this example of the invention, when the PDI system 100 thus receives such a request from an electronic merchant 202, the PDI web-enabled server 204 invokes the Filter Manager 208 by means of a CGI program or script. Generally, this process is the first process for user authentication, and determines the legitimacy of the PDI request for service. The Runtime Config file 402a specifies the business rules used by the Filter Manager. The PDI system 100 is preferably configured to allow or deny certain electronic storefronts from using the PDI system directly. Accordingly, as the Filter Manager 208 receives a request, the merchant domain identity is evaluated (block S402). This identity can be in the form of the HTML/CGI REFERER field as populated by the web browser 102c, or can be a specialized form element, PDI_MERCHANT, that is populated directly by the storefront prior to transmission. In either case, the merchant must identify itself to the PDI system through domain notation, or through private PDI tokens. Once the identity of the merchant site is determined, the Filter Manager 208 consults a specialized business rule file, ESITES 402f. This file lists all of the merchant domains from which PDI requests will be accepted. This allows the owner of the system to process requests only from specific storefronts that are subscribers to the user authentication services of PDI. The ESITES file also lists any special form mapping requirements or default payment gateway servers that are associated with individual storefronts directly. This will be discussed in more detail below.

In addition to filtering electronic storefront domains, the Filter Manager 208 includes functionality for filtering request data as it is associated with Internet Service Providers, or entities offering Internet connectivity. Two additional configuration files, IP.deny 402e and DOMAIN.deny 402d define those IP addresses and/or domain names whose online purchase transaction requests should not be accepted. The format of these files allow the owner of the PDI system to wildcard both domain names and IP addresses. For example, the element 192.6.* would specify any IP address beginning with the quadruples 192.6, followed by any other address elements. Likewise, domain names may be in the form *.name.com, allowing for masking at any domain level. In this latter example, *.name.com would match ip1.name.com, ip2.name.com, or name.com, since all end in the name.com notation. These files are typically populated with Internet Service Provider addresses/domains that have exhibited fraudulent activity in the past, or have been associated with online fraud in some fashion.

The IP.deny file 402e is queried first, and matched against the HTML/CGI REMOTE_ADDR field input to the CGI program as is known in the art (block S404). If a match is found, the purchase request is immediately redirected to a dynamic error page and displayed on the Client browser 102c. As a result, the purchase request will never be fulfilled. After the IP.deny file 402e is queried, the same operation is performed on the DOMAIN.deny file 402d, using data matched against the HTML/CGI REMOTE_HOST input field (block S406). As is the case with address matching, domain matching will generate the same type of dynamic error page to the Client browser 102c and stop the transaction from continuing if a match occurs.

If an incoming purchase request is not specified in either of the denial files, it may continue to the next stage of processing. Preferably, the PDI system is designed to allow easy integration with existing payment gateway services, such as CyberCash, TransAct, IPAY and many others. In order to accomplish this, a mapping between the form elements required by the gateway protocols and the electronic storefront should be established. The Filter Manager 208 process uses the existing ESITES file 402f to find any specialized mapping file which is associated with a given storefront. For example, all storefronts using the PayDirect gateway service would specify the same local mapping file, whereas CyberCash-enabled storefronts would point to a different local file. The mapping files are nothing more than form element names, and their relationship to PDI form tokens. For example, merchant accounts might be specified with text such as "Estore1.com uses /filepath/paydirect.data," which indicates that an electronic storefront at domain Estore1.com uses a mapping file paydirect.data located in a /filepath directory or subdirectory.

After the Filter Manager 208 determines which localized "mapping" form file is associated with the merchant, it is read into memory (block S408). This file is a list of relationships, which determine the physical names used by the merchant to specify purchase parameters. For example, one storefront may regard a customer's first name as FNAME=<value> in specifying data to the payment

gateway; others may use elements such as FIRST_NAME=<value>. The associated mapping file creates the relationship between what the merchant calls a token, and its corresponding PDI system 100 internal reference. For example, the following entry may exist within a particular mapping file: PDI_FIRST_NAME = FNAME, PDI_LAST_NAME = LNAME. This entry identifies the first name field within the form as using the FNAME token to describe it, and the LNAME form element to identify the last name of the consumer. In this fashion, the PDI system 100 can support different variations of form descriptions, regardless of the token name used to represent that element. If no mapping file is specified for a particular electronic storefront, the Filter Manager 208 system reads default form tokens from the Default Registration File 402g.

If the Filter Manager 208 in block S408 finds a valid form-mapping file, then transaction processing can continue. If, however, a mapping relationship cannot be established between the merchant form and the internal PDI tokens, a dynamic error page is created and sent to the Client browser 102c. This error message can instruct the consumer to contact the merchant site for additional support, since its protocol to the PDI system 100 is not properly supported.

After the Filter Manager 208 performs token translation, a check is made to ensure that all required form elements are actually present (block S410). The PDI system 100 requires that a minimum set of identity parameters be specified in any purchase request, so that the consumer's registration record can be retrieved. These fields can include the consumer's first name, last name, billing address, street, city, state, etc. If any of these form elements are missing, the business rules of the system determine the next course of action, as will become apparent below.

If the PDI system 100 is configured by business rules to augment missing form elements (determined in block S414), then it dynamically creates an HTML page 404a, which lists and requests those missing identity form elements from the consumer. The form elements which are given in the original request are made part of the dynamic HTML page in the form of hidden elements, so that resubmission of the form by the Client browser 102c contains all identity elements (new plus previous) (block S416). The customer is then requested to supply the missing elements (block S418). Receipt of the missing data is redirected back to the PDI system 100 for processing (block S420). If the PDI system 100 is configured by business rules to not augment missing fields, a dynamic HTML error page is constructed and returned to the Client browser 102c, indicating that the transaction cannot proceed (block S422).

Once all form elements are present (determined in block S410), then they are parsed into their separate token/value pairs and stored in memory (block S412). This data becomes the input to the Identity Manager 210 process S502.

FIG. 5A outlines components that comprise, or are accessed by, the Identity Manager 210. Generally, the Identity Manager service is responsible for ensuring that a consumer has been PDI registered and is properly enrolled within the PDI System 100, and retrieves consumer context for

downstream processing. As shown in FIG. 5A, several configuration files 402 are accessed during processing by the Identity Manager 210. As will be described in more detail below, the contents of these files determine this manager's business rules and configuration (Runtime Configuration Data 402a), Data Storage 220 access methods (Data Store Security 402b), and rules and procedures for data transformation and standardization (Dictionary Data 402h and Address Rule Data 402i).

FIG. 5B is a diagram illustrating an example of the processing flow for Identity Manager 210. In the present example, the Identity Manager 210 is entered after the Filter Manager 208 has extracted and parsed identifying data related to the current transaction (block S502). The Identity Manager 210 first utilizes this data to determine if sufficient information is available to accurately identify the consumer (block S504). If sufficient information is not available, the request is redirected to a Missing Registration HTML Page (block S506) that allows the consumer to augment and provide required data. If the missing information is due to the consumer not being registered with the system (or not having sufficient registration information), the client browser may be alternatively directed to a system registration process (see block S602 in FIG. 6).

If the request and extracted data contain all of the components required by the PDI System 100 for identity verification (determined in block S504), the rules and procedures for data transformation and standardization found in the Dictionary Data 402h and the Address Rule Data 402i are utilized to create an appropriate Subscriber Data 420a query. The appropriate query is then invoked against the Subscriber Data 420a within the Storage System 220 to retrieve the "represented" consumer's record and associated template. If the query in block S507 fails, a dynamically augmented rendering of a system configured Error page S508 is returned to the Client 102.

If a unique registration entry is found in block S507, then a determination is made as to whether the consumer has previously and successfully registered (PDI_REGISTERED), which indicates that either an administrator via Administrative Services component 218 pre-registered the individual, or that the individual has attempted registration previously via that or another process. The process then determines if the consumer is properly enrolled within the PDI System 100 (block S510). "Properly enrolled" implies that the consumer has a registered DigitalCode and/or biometric template for authentication comparison. If the consumer is not properly enrolled with the PDI System 100, the request is redirected to the PDI web-enabled Server 204 with appropriate result code. If the consumer is properly enrolled as determined in block S510, and required templates are available, the Identity Manager 210 then determines whether the consumer is Blacklisted (block S512). The Blacklist contains a list of consumers whose transactions/requests are to be immediately denied by the PDI system 100. If the consumer information exists in the PDI Blacklist then the appropriate result code (DENY) is returned to PDI web-enabled server 204 to take appropriate action. If the consumer information is not contained on the PDI Blacklist then the request is forwarded to the Transaction Rules Manager for further processing and authentication determination (see block S702 in FIG. 7B).

FIG. 6 is a diagram illustrating an example of the flow of processing for the Registration Process within the PDI System. In one example of the invention, by way of the client web browser 102, the consumer submits required form data to an Electronic Storefront 202 for the purchase of goods and authorization by the Credit Payment Network 206. The request and form data are forwarded to the PDI web-enabled Server 204. The PDI web-enabled Server 204 then determines if templates exist for the consumer by way of the Identity Manager 210 before further processing is conducted against the request. If the Identity Manager cannot locate consumer personal information and/or templates for the current request, the consumer is redirected to a Registration Page if so configured by the business rules of the system, thus initiating the registration process described below.

As shown in FIG. 6, PDI System 100 first determines if the request is submitted from a valid electronic storefront 202 (block S602). If PDI system 100 cannot validate the site, the consumer is redirected to a Dynamic HTML Page so alerting the consumer (block S604). If the request is submitted from a valid site (determined in block S602), the request and form data are then cleansed for PDI Processing (block S606), ensuring that all of the form data that is provided by the client can be reformatted to a standard format used by the PDI system. For example, "123 Main Street and 123 Main St. are the same address which would be cleansed to "123 Main St." by the PDI system 100. Once the form data is extracted, the corresponding session must be located and read. If the form data submitted by the consumer could not be mapped and cleansed (determined in block S606), the consumer is redirected to a Dynamic HTML Page (block S604). If the form data are properly cleansed and mapped, the PDI System then determines if all required components are available within the form data (block S608). If required components are missing, the consumer is advised and requested to submit those form data by way of a Dynamic HTML Page (block S604). If the request and form data contain all required components for PDI Processing, then the PDI system uses an Enrollment Key, e.g. a unique string of characters sent to an individual, to determine which consumers are authorized to register within the system (block S610). The Enrollment Key identifies the consumer as a legitimate participant of the PDI system 100 and can be sent via e-mail, regular mail, and/or other acceptable means that ensure that the Enrollment Key is not compromised. If the Enrollment Key provided by the consumer is not valid, the client 102 is redirected to a Dynamic HTML Page (block S604). If the Enrollment Key is validated in block S610 by the PDI system 100, the system continues processing the request by way of the Registration Process.

Once all required components are deemed available (block S608) and a Valid Enrollment Key has been provided (block S610), the PDI system 100 then determines if the consumer exists within the PDI system 100 using submitted form data (block S612). If the consumer exists within the PDI system 100, the consumer is redirected to an Update Personal Options page (block S614), which page allows the registered consumer to Update, Add, and/or change personal information that is stored within the Data Storage Subsystem 220.

If the consumer does not exist within the PDI system 100 as determined in block S612, the form data that is associated with the request is inserted into the PDI System 100 (block S616) and the Registration Process continues. After the newly collected consumer information is inserted into the PDI System 100, the process determines if the client 102 is equipped with the PDI Client Software 102d (block S618). If the PDI Client Software 102c is not available, the consumer is requested to provide a Digital Code (block S622) that will be updated to the consumer record for future authentication (block S630).

If the PDI Client Software 102c is available as determined in block S620, the consumer is prompted to enter a Digital Code (block S624) (e.g. a secret word or pass-phrase that an individual uses to gain access or admittance to a computer and/or information), and after successful collection of the Digital Code, the process invokes the PDI Client Software (block S626), in order to collect the biometric template from the consumer. The consumer provides the biometric template by way of the Biometric Collection Device 102b in block S628. After the Digital Code and biometric template have been successfully collected from the consumer and verified for accuracy, the consumer record is updated (block S630). After the PDI System 100 updates the consumer record, the request is redirected to a Dynamic HTML page (block S604), as configured by the business rules of the system.

FIG. 7A illustrates the high-level data components utilized by the Transaction Rules Manager 212 according to one example of the invention. Generally, the Transaction Rules Manager 212 is responsible for processing the client's request against company level (i.e. business) rules to determine if authentication is required and, if so, what type of authentication should be requested of the consumer. As shown in FIG. 7A, several configuration files 402 are used during processing by the Transaction Rules Manager 212. As will be described in more detail below, the contents of these files determine this manager's business rules and configuration (Runtime Configuration Data 402a), Data Storage 220 access methods (Data Store Security 402b), HTML templates for dynamic rendering of error notifications (Template HTML File 404), and associated subscriber (Sub Data 420a), transaction (Transaction Data 418a), base (Base 414), link (Link 416) and rule (Active Rules 410a-g) data stores within the Storage System 220.

FIG. 7B is a diagram illustrating an example of the processing flow for Transaction Rules Manager 212. As shown in FIG. 7B, upon entry, the monetary amount of the current transaction is checked against the configurable System Maximum Allowable Amount (block S702). If the Monetary Amount exceeds the System Maximum Allowable Amount, then a redirection request to a configurable dynamic web page is returned to the Client 102 via the PDI web-enabled server 204 (block S734). If the Transaction Monetary Amount does not exceed the System Maximum Allowable Amount, then processing continues by checking whether Consumer Imposed Registration Limits exist (block S704).

If Consumer Imposed Registration Limits do not exist, then processing proceeds to Push and/or Retrieve Transaction Relationship (block S710). If the Consumer Imposed Registration Limits exist, then the monetary amount of the current transaction is tested (block S706), and if it exceeds the Per Transaction Limit, then a redirection request to a configurable dynamic web page is returned to the Client 102 via the PDI web-enabled server 204 (block S734). If the Per Transaction Limit is not exceeded, then processing continues by checking whether the Consumer Monthly Limit is exceeded (block S708).

If the monetary amount of the current transaction plus the monetary amount aggregate of the current month's transactions exceed the Consumer Monthly limit, then a redirection request to a configurable dynamic web page is returned to the Client 102 via the PDI Web-enabled Server 204 (block S734); else processing continues to Push and/or Retrieve Transaction Relationship (block S710).

The Push and/or Retrieve Transaction Relationship block S710 stores linkage associated relationships from the current transaction into, and retrieves historical linkage associated relationships from, the Data Storage Subsystem 220. These relationships are used throughout the remainder of the Transaction Rules Manager activities blocks S712-S730.

After the relationships have been retrieved from the Data Storage Subsystem 220 (block S710), Global Constraints are then retrieved from the Data Storage Subsystem 220 (block S712). The Global Constraints are then examined to determine if a Global Authentication Method is mandated (block S714). If mandated, then processing flows to PDI Authentication Determined block S732; if not, then processing continues by setting the authentication method to PDI_AUTH_NONE (block S716) before proceeding to evaluate Network Constraints (block S718).

As shown in FIG. 7C, Network Constraints are evaluated in block S718 by retrieving the associated constraint vectors from the Data Storage Subsystem 220. If the current transaction matches the logic of one of the constraint vectors, then the associated authentication method is selected, and if more strict than the current authentication method, the current authentication method is updated (block S720). If the current authentication method was updated and now equals the maximum authentication available, then flow proceeds directly to PDI Authentication Determined (block S732); else flow continues by evaluating Identity Constraints (block S722).

Identity Constraints are evaluated by retrieving the associated constraint vectors from the Data Storage Subsystem 220 (block S722). If the current transaction matches the logic of one of the constraint vectors, then the associated authentication method is selected, and if more strict than the current authentication method, the current authentication method is updated (block S720). If the current authentication method was updated and now equals the maximum authentication available, then flow proceeds directly to PDI Authentication Determined (block S732); else flow continues by evaluating Boolean Constraints (block S724).

Boolean Constraints are evaluated by retrieving the associated constraint vectors from the Data Storage Subsystem 220 (block S724). If the current transaction matches the logic of one of the constraint vectors, then the associated authentication method is selected, and if more strict than the current authentication method, the current authentication method is updated (block S720). If the current authentication method was updated and now equals the maximum authentication available, then flow proceeds directly to PDI Authentication Determined (block S732); else flow continues by evaluating Transaction Constraints (block S726).

Transaction Constraints are evaluated by retrieving the associated constraint vectors from the Data Storage Subsystem 220 (block S726). If the current transaction matches the logic of one of the constraint vectors, then the associated authentication method is selected, and if more strict than the current authentication method, the current authentication method is updated (block S720). If the current authentication method was updated and now equals the maximum authentication available, then flow proceeds directly to PDI Authentication Determined (block S732); else flow continues by evaluating Purchase Constraints (block S728).

Purchase Constraints are evaluated by retrieving the associated constraint vectors from the Data Storage Subsystem 220 (block S728). If the current transaction matches the logic of one of the constraint vectors, then the associated authentication method is selected, and if more strict than the current authentication method, the current authentication method is updated (block S720). If the current authentication method was updated and now equals the maximum authentication available, then flow proceeds directly to PDI Authentication Determined (block S732); else flow continues to Behavior Constraints (block S730).

Behavior Constraints are evaluated by retrieving the associated constraint vectors from the Data Storage Subsystem 220 (block S730). If the current transaction matches the logic of one of the constraint vectors, then the associated authentication method is selected, and if more strict than the current authentication method, the current authentication method is updated. Flow continues to PDI Authentication Determined (block S732).

Once PDI Authentication has been determined S732, flow continues to the User Profile Manager 214.

FIG. 8A illustrates the high-level data components utilized by the User Profile Manager 214 according to one example of the invention. As shown in FIG. 8A, User Profile Manager 214 accesses several configuration/parameter files during processing. As will be explained in more detail below, these files establish the business rules of the PDI system 100, and determine which (and how) transactions will be processed by PDI. Temporary files are used to store transaction form data, until the necessary user authentication has been validated by the system. Encryption keys are also stored in temporary storage areas, since they are valid for a single session only. In addition, template HTML files may be used to construct error messages, or information collection messages back to the Client

browser 102c as necessary. Data storage is handled by a series of database tables, which access profiling information, store transaction elements and create linkage relationships between the current transaction and its associated network elements.

FIG. 8B is a diagram illustrating an example of the processing flow of User Profile Manager 214 within the system architecture of the present invention. Generally, this subsystem is responsible for evaluating the current transaction for authentication needs, by using behavioral-based profiling algorithms as described below. In the present example, input to the User Profile Manager 214 is in the form of a previously evaluated user authentication method to be applied to the current transaction, as determined by the Transaction Rules Manager 212.

Authentication inputs received from the Transaction Rules Manager 212 may be, for example, any of the following identifiers: PDI_AUTH_NONE, identifying that no matching rules were evaluated in prior steps; PDI_AUTH_ALLOW, indicating that the transaction should be allowed without further evaluation; PDI_AUTH_DC, indicating that a DigitalCode should be used to authenticate the individual; PDI_AUTH_BEST, indicating that the best method available on the Client 102 should be used, depending upon availability of the Biometric Collection Device 102b; PDI_AUTH_FP, indicating that a biometric fingerprint should be used to authenticate the individual; PDI_AUTH_FP_DC, indicating that both a DigitalCode and biometric fingerprint should be used to authenticate the individual; and finally, PDI_AUTH_DENY, indicating that the transaction should be denied completely.

The business rules of the PDI system 100 determine whether or not behavioral-based processing should proceed, even when an authentication method is directly specified by the Transaction Rules Manager 212. Business rules for the system are defined by the Runtime Config File 402a, which identify the runtime parameters that are applied during transaction analysis. If it is determined that the specified authentication method currently input is the highest level available (namely, PDI_AUTH_DENY), no additional processing occurs, since behavioral-based evaluation would be unable to supersede the method previously input (block S802). If, however, business rules dictate that behavioral-based profile processing should be applied in conjunction with input authentication methods, or, if no authentication method was previously determined (PDI_AUTH_NONE), then profiling algorithms are deployed (block S804).

The evaluation of historical transaction relationships for the individual subscriber is extracted from the linkage tables of the PDI system 100, where they are evaluated (block S806). The User Profile Manager 214 maintains a unique relationship between all network elements that comprise a transaction, and associates this data directly to the individual requesting that transaction. Access to these relationships is through the Data Store Security File 402b, which defines the security access parameters to the Data Storage System 220.

The PDI system 100 is preferably designed to allow the addition or deletion of network elements, depending upon the deployment environment. In the case of electronic commerce transactions, network elements are maintained on a per-individual basis, and an occurrence count is incremented each time a transaction isolates the usage of an identifiable network element. In addition, for each element the system maintains a historical count of the number of times the element has been successfully authenticated, as well as the number of times that element is associated with a transaction whose authentication request has failed. In this fashion, each individual network element has its own "score" maintained in an atomic fashion, depending upon previous authentication attempts. As more transactions are processed for a particular individual's purchase requests, the authenticity of a given element as associated with that individual is bolstered.

For example, the use of an IP address by an individual five times would cause a count of both successes and failures totaling five to be maintained by the system. The distribution of the success versus failure counts indicates the current score of the individual network element for that individual's previous purchase patterns. In the case of an individual who has used IP address 206.168.56.5 five times in the past, a distribution of a success count of four times and failure count of one time (totaling five) would be scored as $4/5 * 100 = 80\%$. As a result, the IP address linkage for the individual using 206.168.56.5 indicates that 80% of the time in the past, successful authentication has occurred when transactions originated from this service provider address.

Network elements, as used herein, include such components as IP address, electronic storefront domain name, shipping address, contact information, browser software, credit card information, transaction amount, time-of-day, and day-of-week, etc. This list is intended as illustrative rather than limiting and other components will be apparent to those skilled in the art. Network elements are stored in the Data Storage Subsystem 220, and are associated directly with the subscriber identity record. Each of these vectors has direct linkage relationship with the individual consumer's registration data, and historical usage counts (occurrences, successes, failures) are maintained for each network element used by the consumer in the past. In this fashion, the profiling algorithms of the PDI system 100 are able to evaluate the usage score of each network element as it pertains to the individual, and compute aggregate scores based upon the combination of all network elements seen in the current transaction.

In order to allow administrators of the PDI system 100 to customize the manner in which scores are computed for any given transaction, each network element has an associated weight constant that is applied during analysis. This weight is defined in the business rules configuration file, and determines what "strength" should be applied to all network elements within the system. In this fashion, system administrators can determine which transaction components should be regarded as more important within the target environment, based upon historical fraud patterns or availability of certain components in general.

As each network element of the current transaction is evaluated and weighted, an aggregate score is computed based upon historical authentication patterns of the target individual consumer. This score represents the overall historical authentication certainty as it pertains to an aggregation of network elements associated with the claimed individual. In general terms, the final score is computed by comparing the total number of times a given network element has been successfully authenticated, and dividing that value by the total number of attempts to that network element. This in turn, yields an authentication percentage. Each network element is multiplied by the weight value assigned to that element, to determine the overall score for the particular element. The summation of all these scores is then divided by the sum of the weights. The final score is a percentage, in the range of 0 – 100.

Upon completion of this process (block S808), the authentication score is compared to the business rules established by administrators of the PDI system 100. These business rules specify threshold values that pertain to specific authentication methods to apply. For example, the business rules of the system may specify that scores between 80% and 85% should require the given transaction to be authenticated by means of a Digital Code. This information is retrieved from the Behavior Data file 402j.

The resultant authentication method returned from behavioral-based processing, as outlined above, is compared to the input authentication method specified by the Transaction Rules Manager 212. The more stringent of the two authentication methods is identified, and becomes the preferred authentication method to apply to the current transaction (block S810).

Upon completion of authentication method analysis, the current transaction is inserted into the Data Storage Subsystem 220 (block S812). At this point in the process, the transaction status is identified, based upon what user interaction is required between the PDI system 100 and the Client 102 machine. Transactions that require no interaction, namely, PDI_AUTH_ALLOW or PDI_AUTH_DENY are regarded as being completed in nature, since no authentication credentials are required. All other transactions, namely PDI_AUTH_BEST, PDI_AUTH_FP, PDI_AUTH_DC and PDI_AUTH_FP_DC require input from the individual in order to verify user identity. These transactions are marked as incomplete in nature since status has not yet been determined, and authentication credentials not yet collected. Each and every transaction in the PDI system 100 is saved, and the associated authentication method, completion status, linkage to network components and reason for authentication is made part of the transaction entry.

As described above, certain authentication methods require interaction between the PDI system 100 and the Client 102, for the purpose of collecting identity credentials. An evaluation is made to determine if such an interaction is required (block S814), based upon the identified authentication steps outlined in blocks S802 and S804. The collection of biometric data, Digital Codes, or the combination of the two is regarded as an interactive process. If, however, the

authentication method is a PDI_AUTH_ALLOW (as determined in block S816), no identity collection is required, and the transaction is immediately forwarded to the credit payment system or external entity as specified by the electronic storefront (block S818). All purchase form data, as originally presented to the PDI System 100, and stored in temporary Form Element Data Files 406b, is forwarded unaltered. In this scenario, the PDI System 100 is merely a pass-through subsystem and appears transparent to the electronic commerce purchase transaction.

If, on the other hand, the authentication method is a PDI_AUTH_DENY (determined in block S820), a denial message is immediately returned to the electronic storefront and no further processing is performed (block S822). The business rules of the system determine if a response code is generated for return to the electronic storefront, or if another URL is invoked instead. If, however, the final path for a non-interactive authentication method is not the result of a deny or accept transaction condition, this indicates that a programmatic problem has occurred within the PDI System 100. The consumer is thus redirected to an error page by the Client browser 102c (block S824).

As indicated previously, certain authentication methods require interaction with the consumer. When such an authentication method is specified (determined in block S814), a determination is made as to which URL will be mapped to the Client browser 102c system for collecting identity credentials.

Turning now to FIG. 8C, therefore, if PDI_AUTH_DC is specified (determined in block S826), then the target URL for collecting identity credentials is marked as DC, specifying Digital Code collection (block S832). A Digital Code will always be on file for a consumer, since the PDI Registration Process described above will not allow a registration record to be inserted into the Data Storage Subsystem 220 unless a valid Digital Code is collected and verified.

If PDI_AUTH_FP_DC is specified (determined in block S828), then a combination of Digital Code and biometric data is to be requested. In order to ensure that this type of authentication is valid, the consumer's registration record is queried to determine if a biometric template is on file (block S830). If such a template is found, the target URL for collecting identity credentials is marked DC (block S832), since Digital Code collection will occur first when multiple credential collections are specified. If, however, a biometric template is not on file for the consumer, a redirection occurs for the purchase request, since authentication cannot be completed due to lack of biometric registration data (block S834). The business rules of the system determine the location of this URL redirection.

The same process is applied to PDI_AUTH_FP (as determined in block S836); if biometric authentication is required, the consumer's registration record is queried to determine if a template exists (block S838). If such a template is found, the target URL for collecting identity credentials is marked as BIO (block S840). As in the PDI_AUTH_FP_DC example, if no biometric template is available, the PDI system 100 redirects the purchase request to the appropriate URL as determined by system business rules (block S834).

Finally, if PDI_AUTH_BEST is specified (determined in block S842), a check is made to determine if a biometric template is available for the consumer (block S844). However, lack of such a template does not generate an error redirection. Rather, if Digital Code is the only information on file for the consumer (block S846), then the target URL for collecting identity information is marked as DC (block S832). On the other hand, if a biometric template is available (block S848), then the target URL is marked as BIO (block S840).

Upon completion of determining the appropriate URL to be mapped to the Client browser 102c for collecting identity credentials, session keys are preferably generated for biometric authentication (block S850). Using public key cryptography (asymmetric encryption), the User Profile Manager 214 generates two keys – a public key and private key (block S850). These keys will be used to encrypt and decrypt biometric data as it is collected and returned to the PDI system 100 for transaction authentication. The size and algorithm to be used in creation of public/private key pairs is specified by the business rules of the system.

The public key generated is included in the URL data to be sent to the Client Browser 102c, so that it may be used to encrypt biometric data prior to transmission back to the PDI system 100. This is accomplished by dynamically updating the BIO URL contents, and adding the public key data as part of the plug-in input parameters. The private key on the other hand, is stored in a protected directory on the PDI system 100, and whose file name is made available to session data that is saved (block S852). This constitutes the temporary Private Key Data file 406a.

Session data 418b identifies the transaction that is currently requiring authentication, and includes details of the transaction state. The session record identifies the authentication method being applied, the IP address from which the current request originated, the date/time that the authentication request was started, the private key file name if biometric collection is occurring, the original purchase form elements sent by the electronic storefront, and the status of any retry attempts from the consumer. Each session record is assigned a unique, non-repeating key value that identifies it from all other session records within the PDI system 100. It is this key that will be used to correlate the current transaction request with authentication responses received from the Client 102 after identity credentials are collected. The session key is appended to the target URL after it is generated, and is stored in the Session Data table 418b on the PDI host.

After session data has been stored within the PDI system 100 (block S852), a dialog is initiated between the PDI web-enabled server and the Client browser 102c. The PDI system 100 redirects the consumer to the previously determined target URL, which begins the credential collection process (block S854). All transactions back to the client are through the PDI web server (block S856). At this point, control is relinquished by the PDI system 100 and the transaction request is still in an incomplete state until identity credentials are received and verified by the PDI system 100.

FIG. 9A outlines components that comprise, or are accessed by, the Authentication Manager 216 in accordance with one example of the invention. Generally, this subsystem is responsible for validating user identity credentials that are passed to the PDI System 100 in response to authentication requests previously sent to the Client workstation 102. For example, if it is determined that a given transaction requires the submission of biometric or Digital Code data, the Client workstation 102 sends the corresponding identity responses to the Web Enabled PDI Server 204, where they are processed directly by the Authentication Manager 216.

As shown in FIG. 9A, several configuration files are used during processing by the Authentication Manager 216, which files specify the business rules of the system, and are explained in greater detail below. Generally, temporary data files 406 are used by the Authentication Manager 216 for the storage of encryption key data and form element data; log files 406 are used to record system messages, errors and processing exceptions; template HTML files 404 identify specific error pages which are mapped to the Client workstation 102 if required; and the Data Storage System 220 maintains the session, transaction, biometric and linkage information for the consumer transaction in progress.

FIG. 9B is a diagram illustrating an example of the processing flow for Authentication Manager 216. As shown in FIG. 9B, upon entry, the HTML form data passed by the Client workstation 102 is extracted and parsed (block S902). This form data preferably contains pre-defined tokens that identify the type and value(s) of authentication information being presented, so that data availability can be determined (block S904). For example, a token such as "DC=<value>" might identify a Digital Code element, and its corresponding value. Likewise, biometric data would include the biometric stream, its byte length and the number of samples being sent, for example: BIO=<value>, BIO_LENGTH=<value>, BIO_SAMPLES=<value>.

If form data cannot be read, or the data passed to the Authentication Manager 216 is deemed corrupt or malformed, a dynamic error page is created for return to the Client workstation web browser 102c (block S906).

Once form data is extracted, the corresponding session must be located and read (block S908). Session data identifies a previously started electronic commerce transaction that required the receipt and validation of authentication credentials. Session information is stored by means of a hidden form element passed back and forth between the Web Enabled PDI Server 204 and the Client workstation 102, normally in the form SESSION=<value>. The session key <value> acts as the lookup mechanism for locating session information directly. If the session information can be found for the current transaction, then further processing may continue.

If session data cannot be found for the current transaction (as determined in block S908), a dynamic web page is constructed, based upon the error, and returned to the Client workstation browser 102c (block S906). Dynamic error page creation can be achieved by a variety of industry-

available techniques, such as Active Server Pages (ASP), or through means of CGI scripts or programs.

The state of the session is then checked to determine its legitimacy (block S910). Sessions are given a finite expiration time, so that transactions must be completed in a timely manner, even when user authentication credentials are collected and evaluated by the PDI system 100. In order to prohibit cutting-and-pasting of source data to the web enabled PDI server 204, authentication responses to the system must be completed within a pre-determined period of time. The business rules of the system, as detailed in the runtime configuration file 402a, determine the length of this "expiration period". Transactions that have "timed-out" are redirected to dynamic web pages, which detail the error to the Client workstation 102 (block S906). A typical value for such a timeout might be in the range of 1 – 5 minutes, depending upon the authentication credentials normally collected. Since user authentication is interactive in nature, this value must be long enough to allow a dialog (or dialogs) to complete over networks such as the Internet, but not so long as to allow transactions to be cut-and-pasted by potential hackers.

Like session timeout validation, IP address validation is also conducted. When a session is created and stored by the User Profile Manager 216, the IP address of the original transaction is stored as part of the session data. As authentication requests are matched to their corresponding sessions, the original IP address is compared to the current IP address of the transaction. If the client IP addresses match (determined in block S912), then transaction flow is permitted to continue. If, on the other hand, the IP addresses do not match, then a dynamic web page is constructed and returned to the Client workstation 102 (block S906). As in the case of session expiration, IP address mismatching does not permit the transaction to continue. IP addresses that do not match are potential cut-and-paste operations, which may indicate an attempt to circumvent the presentation of valid user credentials. It is understood that there are multiple reasons for such an event occurring, such as client Internet service disconnects/reconnects. Regardless of the reason, IP address matching is determined by the business rules of the system, and when specified, must match exactly before transaction processing will be allowed to proceed.

The type of user authentication is then determined by the form elements presented (determined in block S914). If the authentication contains Digital Code credentials, then a direct comparison between the presented Digital Code and the Digital Code stored as part of the user identity record is performed (block S946). As shown in FIG. 9C, if the digital codes match, then transaction processing continues, as will be described below. If, however, the Digital Code data does not match, the business rules of the system are consulted to determine the number of retries an authentication request is allowed. If the number of retries has not been exceeded (as determined in block S948), the current transaction record is updated to indicate that a failed Digital Code authentication has occurred (block S956). The corresponding session record is also updated (block

S958), decrementing the number of additional attempts which will be permitted based upon the system business rules. The session timeout is also refreshed, allowing retry attempts to function as though the session were started anew (block S958). Upon completing these updates, a dialog is re-initiated between the PDI web server 204 and the Client browser 102c (block S960).

5 If, on the other hand, the number of retries has been exceeded with respect to Digital Code collection, the transaction relationships between the network elements are updated, and marked as 'authentication failures' (block S950). For example, if the current transaction has a linkage relationship to IP address 206.168.56.6, the individual subscriber's data record would be updated to indicate an incremented failure from this Internet address. This type of selected network element
10 success/failure counting on a per-individual basis allows the User Profile Manager 216 to perform adaptive authentication profiling.

Scenarios which exceed the maximum number of retries without presenting valid Digital Code credentials will automatically delete the session record associated with the current transaction (block S952), and generate a dynamic error page to the Client browser 102c, indicating that the
15 transaction could not be authenticated. As a result, the original purchase request is never routed to a payment system, thus canceling the transaction.

Upon successful matching of Digital Code credentials to registered values (block S946), processing continues to further determine if user authentication has been completed. Since the PDI system 100 allows for a combination of credentials to be collected for a single purchase request (i.e.,
20 PDI_AUTH_FP_DC), a check is first made to determine if biometric authentication is required (block S962). The session record for this transaction contains the necessary authentication method to be applied. If no additional authentication is required, the transaction relationships between the network elements are updated, and marked as "authentication successes" (block S964). As is the case for authentication failures, network element updates on a per-individual basis allows adaptive
25 authentication to evolve and strengthen over time.

Upon successful Digital Code authentication matching, and if no further authentication is required, the final set of data is retrieved from the session record prior to its deletion. The session record maintains the location of the original form elements, as extracted by the User Profile Manager 212, and stored in a temporary file within the Data Storage Subsystem 220 (Form Elements Data File
30 406b). These form elements allow the Authentication Manager 216 to reconstruct the original electronic commerce purchase request, as though the PDI system 100 was never involved in the original transaction. Once this data is extracted and loaded (block S966), the associated session record is summarily deleted (block S968). A CGI script, for example, loads the form data, where it redirects the transaction to the appropriate payment system as specified by the electronic storefront
35 originally (block S970).

If it is determined in block S902 that biometric collection is required upon receipt and validation of Digital Code, then the current transaction is updated to reflect that partial user authentication has completed (block S972). The transaction is still left in an incomplete state, pending the receipt and validation of biometric credentials. Session keys are generated for this authentication request, so that biometric encryption can be achieved (block S974). Session information is also updated, indicating that the Digital Code portion of the request has completed (block S958), and biometric credential collection is now in progress. At this point, a dialog is re-initiated between the PDI web server 204 and the Client browser 102c, asking for biometric data collection (block S960).

Returning to FIG. 9B, like the description of Digital Code collection, the type of user authentication extracted from the HTML form data may indicate that biometric data is being presented (block S914). A comparison of the presented biometric credentials, and those on file for a given consumer must then be conducted in order for transaction processing to continue. Unlike DigitalCode comparisons, however, biometric data is encrypted to protect consumer privacy. The corresponding session record that was located in block S908 identifies the location of the private key file required to decrypt the transmission. This file is the corresponding public/private asymmetric key pair that was generated when the biometric authentication request was originally initiated and is thus retrieved (block S918).

The private key file is extracted from the Data Storage System 220 and used to decrypt the BIO form element received in block S902. The status of the decryption process is evaluated in order to determine if the BIO data has been modified in transmission, or if an attempt has been made to cut-and-paste the information to the Authentication Manager 216 (block S920). Because a unique session key is generated each time a biometric authentication request is generated, only the stored private key is capable of decrypting the resultant message. Randomization ensures that the session key cannot be "guessed" by a potential hacker.

If the biometric data is deemed compromised in any way, a dynamic error message is returned to the Client browser 102, indicating that the electronic purchase transaction has been canceled (block S906). This type of error does not allow retry logic to be invoked, since the system cannot determine the legitimacy of the consumer making the transaction request.

The Authentication Manager 216 retrieves the stored biometric template for the target consumer from the appropriate biometric database (block S922). Biometric data for the consumer must have been previously registered with the PDI system 100, and must be located in a data store accessible to the Authentication Manager 216 process. The physical location of this biometric database is independent of the PDI system 100 design, since it may exist within a distributed database or file system environment. The Authentication Manager is preferably capable of making local or remote network requests to an industry-standard relational database that can be housed anywhere within the network environment.

Once the biometric template is recovered for the consumer, it is compared to the presented biometric credentials (block S924). Threshold matching for biometric data is defined by the business rules of the system, and is used to determine the certainty level acceptable to the PDI owner.

Threshold matching typically is expressed as a ratio of certainty, such as 1 in 1 million or 1 in 500 (1:1000000 or 1:500). This certainty level is used to determine the pass/fail status of the biometric comparison.

If a biometric match is encountered (determined in block S926), the transaction relationships between the network elements and the consumer are updated, and marked as "authentication successes" (block S928). The form data saved for the original purchase transaction is extracted from the session data, loaded by a CGI script, and redirected to the appropriate payment system as specified by the electronic storefront originally (block S932). Prior to transmission, the session is summarily deleted (block S930).

Biometric data that does not match the consumer's template (as determined in block S926) causes retry logic similar to Digital Code authentication to be executed. A set number of retries is established by the business rules of the PDI system 100, which controls whether additional user authentication requests should be initiated. If the number of retries is exhausted (as determined in block S934), then the transaction relationships between the network elements and the consumer are updated to an "authentication failure" status (block S942), indicating that none of the transaction components could be authenticated. The session is then deleted (block S944), and a dynamic HTML page is sent to the Client browser 102c indicating that the transaction has been halted (block S906).

If the number of retries has not been exceeded (as determined in block S934), the current transaction record is updated to indicate that a failed biometric authentication has occurred (block S936). The corresponding session record is also updated, decrementing the number of additional attempts which will be permitted based upon the system business rules (block S938). The session timeout is also refreshed, allowing retry attempts to function as though the session were started anew. Upon completing these updates, a dialog is re-initiated between the PDI web server 204 and the Client browser 102c (block S940).

FIG. 10 is a diagram illustrating an example of the flow of control for the PDI Client Software 102d, which is installed on the Client workstation 102. Generally, this software allows the workstation to communicate between the PDI web server 204 and the Client browser 102c, through use of standard plug-in or COM interface elements, for the purpose of collecting biometric data.

In one example of the invention, browsers such as Netscape Communicator load the PDI Client Software 102d as a standard plug-in module, which is invoked by the browser in response to MIME types assigned to the PDI system 100, for example. If a consumer's browser does not have the necessary PDI Client Software 102d, the PDI registration process is preferably able to detect this

condition, and can redirect the consumer to the proper web location for downloading and installation instructions.

Invocation of the PDI Client Software 102d in response to assigned MIME types includes data elements sent by the PDI system 100. Because user authentication must be associated with a particular purchase transaction, session information is sent directly to the Client browser 102c, which is in turn passed to the PDI Client Software 102d. For example, the PDI web server 204 initiates a biometric user authentication request on the consumer's computer by specifying a pre-determined MIME type, and passing certain state variables along with the request. These state variables include SESSION, which identifies the context of the purchase transaction and ENCRYPTION, which details the encryption algorithms/key sizes to be applied to the returned data.

The PDI Client software 102d of the present invention preferably includes functionality supporting the collection of user authentication credentials. Depending on the nature of the credentials requested from the PDI system 100, the PDI Client software 102d may be required to communicate with hardware devices on the Client workstation 102. For example, the PDI system can be configured to acquire fingerprint biometric data directly from the consumer's hardware collection device 102b. In this situation, the PDI Client Software 102d would control a fingerprint reader directly. In contrast, the PDI system 100 may require simple user authentication, such as the supply of a Digital Code, which would be collected through standard HTML form input.

As shown in FIG. 10, in response to the MIME type application/x-pdi (file extension pdi), for example, an attempt is made to load the PDI Client Software 102d by web browser 102c. If the appropriate plug-in module cannot be found, or cannot be loaded correctly due to version mismatches (determined in block S1002), the browser is instructed to redirect the consumer to a PDI-controlled location for the purpose of downloading the client software (block S1004). Once downloaded and installed, the consumer must restart the browser in order to continue (block S1006).

Once the appropriate PDI plug-in module is loaded by the browser (block S1008), an internal check is conducted to determine if communication between the PDI software and the biometric hardware device 102b is working correctly. This involves the opening of driver files which control the hardware unit (block S1010). If the drivers cannot be properly opened, a status message is immediately returned to the PDI web server 204 (block S1012). This feedback is used to inform the consumer that user authentication cannot continue due to hardware or software errors on the Client computer 102. Error data such as this may also be used to facilitate reporting of problem devices, and to allow customer care to address installation problems encountered by a base of consumers.

Successful communication between the biometric device 102b and the PDI Client Software 102d is checked, to ensure that the device is responding to capture and identity requests (block S1014). If this communication fails, or if errors are detected, the same status messaging between the

PDI web server 204 and the software is initiated as described above. For example, a unique status code can be returned to the PDI system, detailing the nature of the error encountered (block S1012).

Biometric collection of the hardware 102b unit is initiated by the present invention after all validation checks have completed normally (block S1016). This process presents a feedback
5 mechanism to the consumer directly within the current web page being viewed, or maps a separate window on the Client workstation 102. This feedback mechanism shows the consumer the current fingerprint image being presented on the hardware unit, as well as pressure and coverage parameters. This feedback data allows the consumer to adjust finger position, pressure sensitivity, coverage placement, etc., based upon the information provided by the PDI Client Software 102d. Because the
10 presentation of fingerprint biometric data often requires practice on the part of the consumer, this feedback data allows the individual to more easily learn to use the hardware device.

The present invention also allows the consumer to abort a current biometric collection, releasing control of the Client browser 102c from PDI. Aborting a user authentication request, however, will send status data to the PDI web server 204 indicating that the authentication process
15 was manually stopped by the consumer (blocks S1018/S1012). A biometric collection that is aborted is regarded as unsuccessful user authentication, and the PDI system 100 determines the next course of action based upon business rules of the system.

Successful collection of biometric data as determined in block S1018 results in encapsulation of the information into minutiae points, which are digital characterizations of the fingerprint
20 information. The manner in which this data is digitally converted is determined by the hardware manufacturer of the biometric unit, and is vendor-supplied. Prior to transmission of this user authentication information, the minutiae points must be encrypted. Encryption is conducted based upon parameters sent by the PDI web server 204, instructing the PDI Client Software 102d as to the nature of the encryption algorithm(s) and key sizes to use (block S1020).

25 Upon completion of the encryption process, the biometric data is forwarded to the PDI web server 204, and includes all original SESSION information contained within the request (block S1022). As a result, this user authentication information is then associated with a particular purchase transaction, allowing evaluation of the submitted credentials to continue.

Although the above discussion refers to an example of the invention where fingerprints are
30 used as the biometric authentication data, it should be noted that other types of biometric and personal identification indicia (i.e. tags) are possible, such as voice patterns, eye patterns (retina or iris), face patterns (e.g. infrared or optical), handwriting, keystroke entry patterns, gait, modus operandi profiles, etc.

The examples of the processing depicted in the above figures is meant to be illustrative rather
35 than limiting. Those skilled in the art, after being taught by the above examples, will appreciate that many modifications can be made to the above methods, including substitution, elimination,

consolidation and re-ordering of many process steps, while remaining within the scope and purpose of the present invention.

Further, although the present invention has been described in detail with reference to the preferred embodiments thereof, those skilled in the art will appreciate that various substitutions and modifications can be made to the examples described herein while remaining within the spirit and scope
5 of the invention as defined in the appended claims.

What is claimed is:

1. A method for reducing the occurrence of unauthorized use of on-line resources, comprising:
 - receiving a message indicating a request from a user to use on-line resources;
 - determining whether the request requires authentication;
 - obtaining an indicia of physical identification from the user if authentication is required;
 - comparing the obtained indicia to a stored indicia for the user; and
 - enabling the request to be fulfilled if the obtained indicia matches the stored indicia.
2. A method according to claim 1, wherein the step of determining whether the request requires authentication includes determining whether a stored profile for the user indicates that authentication is required.
3. A method according to claim 1, wherein the step of determining whether the request requires authentication includes determining whether stored business rules for a company associated with the requested on-line resource indicates that authentication for the user is required.
4. A method according to claim 3, wherein the step of determining whether the stored business rules requires authentication includes:
 - determining whether the user is listed by the company as always requiring authentication; and
 - requiring authentication if the user is listed.
5. A method according to claim 3, wherein the step of determining whether the stored business rules requires authentication includes:
 - determining whether the user is listed by the company as never requiring authentication; and
 - not requiring authentication if the user is listed.
6. A method according to claim 3, wherein the step of determining whether the stored business rules requires authentication includes:
 - determining whether the user is listed by the company as being completely denied access; and
 - completely denying access to the requested on-line resources if the user is listed.

7. A method according to claim 1, wherein the step of determining whether the request requires authentication includes determining whether the request is indicative of fraudulent behavior.

8. A method according to claim 7, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

9. A method according to claim 1, further comprising determining whether the request satisfies other criteria of authorization if authentication is not required.

10. A method according to claim 9, wherein the step of determining whether the request satisfies other criteria includes:

- determining whether the request is a card transaction;
- determining whether restrictions applied to the user and an account associated with the request are satisfied by a purchase associated with the request; and
- denying the request if the restrictions are not satisfied.

11. A method according to claim 10, wherein the restrictions are one or more of type of goods to be purchased, amount of purchase, time of purchase and location of purchase.

12. A method according to claim 9, wherein the step of determining whether the request satisfies other criteria includes:

- determining whether the request is an account transaction;
- determining whether restrictions applied to an account associated with the account transaction are satisfied by the request; and
- denying the request if the restrictions are not satisfied.

13. A method according to claim 12, wherein the restrictions are one or more of frequency of access and time of access.

14. A method according to claim 9, wherein the step of determining whether the request satisfies other criteria includes:

- determining whether the request is an account transaction;
- determining whether use of the requested on-line resources are restricted for an account associated with the user; and
- denying the request if the requested on-line resources are restricted for the account.

15. A method according to claim 9, wherein the step of determining whether the request satisfies other criteria includes:

- determining whether the request is a control transaction;
- determining whether restrictions applied to the user associated with the control transaction are satisfied by the request; and
- denying the request if the restrictions are not satisfied.

16. A method according to claim 15, wherein the restrictions are one or more of a parent control and an other control.

17. A method according to claim 1, wherein the indicia is a biometric.

18. A method according to claim 17, wherein the biometric is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

19. A method according to claim 1, further comprising configuring a set of rules that are used in the determining step.

20. An apparatus for reducing the occurrence of unauthorized use of on-line resources, comprising:

- means for receiving a message indicating a request from a user to use on-line resources;
- means for determining whether the request requires authentication;
- means for obtaining an indicia of physical identification from the user if authentication is required;
- means for comparing the obtained indicia to a stored indicia for the user; and
- means for enabling the request if the obtained indicia matches the stored indicia.

21. An apparatus according to claim 20, wherein the means for determining whether the request requires authentication includes means for determining whether a stored profile for the user indicates that authentication is required.

22. An apparatus according to claim 20, wherein the means for determining whether the request requires authentication includes means for determining whether a stored profile for a company associated with the requested on-line resource indicates that authentication for the user is required.

23. An apparatus according to claim 22, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as always requiring authentication; and

means for requiring authentication if the user is listed.

24. An apparatus according to claim 22, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as never requiring authentication; and

means for not requiring authentication if the user is listed.

25. An apparatus according to claim 22, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as being completely denied access; and

means for completely denying access to the requested on-line resources if the user is listed.

26. An apparatus according to claim 20, wherein the means for determining whether the request requires authentication includes means for determining whether the request is indicative of fraudulent behavior.

27. An apparatus according to claim 26, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

28. An apparatus according to claim 20, further comprising means for determining whether the request satisfies other criteria of authorization if authentication is not required.

29. An apparatus according to claim 28, wherein the means for determining whether the request satisfies other criteria includes:

means for determining whether the request is a card transaction;

means for determining whether restrictions applied to the user and an account associated with the request are satisfied by a purchase associated with the request; and

means for denying the request if the restrictions are not satisfied.

30. An apparatus according to claim 29, wherein the restrictions are one or more of type of goods to be purchased, amount of purchase, time of purchase and location of purchase.

31. An apparatus according to claim 28, wherein the means for determining whether the request satisfies other criteria includes:

- means for determining whether the request is an account transaction;
- means for determining whether restrictions applied to an account associated with the account transaction are satisfied by the request; and
- means for denying the request if the restrictions are not satisfied.

32. An apparatus according to claim 31, wherein the restrictions are one or more of frequency of access and time of access.

33. An apparatus according to claim 28, wherein the means for determining whether the request satisfies other criteria includes:

- means for determining whether the request is an account transaction;
- means for determining whether use of the requested on-line resources are restricted for an account associated with the user; and
- means for denying the request if the requested on-line resources are restricted for the account.

34. An apparatus according to claim 28, wherein the means for determining whether the request satisfies other criteria includes:

- means for determining whether the request is a control transaction;
- means for determining whether restrictions applied to the user associated with the control transaction are satisfied by the request; and
- means for denying the request if the restrictions are not satisfied.

35. An apparatus according to claim 34, wherein the restrictions are one or more of a parent control and an other control.

36. An apparatus according to claim 20, wherein the indicia is a biometric.

37. An apparatus according to claim 36, wherein the biometric is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

38. An apparatus according to claim 20, further means for configuring a set of rules that are used by the determining means.

39. An apparatus for reducing the occurrence of unauthorized use of on-line resources, comprising:

a server that is adapted to communicate with a network based service so as to receive a message indicating a request from a user to use the network based service;

a rules subsystem coupled to the server that determines whether the request requires authentication, and causes the server to obtain an indicia of physical identification from the user if authentication is required; and

an authentication subsystem coupled to the server and the controller that compares the obtained indicia to a stored indicia for the user,

wherein the server sends a signal to the network based service that the request is to be fulfilled if the authentication subsystem determines that the obtained indicia matches the stored indicia.

40. An apparatus according to claim 39, further comprising a database coupled to the controller, the controller accessing historical rules from the database to determine whether authentication is required for the user for a current transaction.

41. An apparatus according to claim 39, further comprising a database coupled to the controller, the controller accessing business rules from the database to determine whether a company associated with the requested on-line resource requires authentication for the user.

42. An apparatus according to claim 39, further comprising a user profile subsystem coupled to the controller which is adapted to determine whether the request is indicative of fraudulent behavior.

43. An apparatus according to claim 42, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

44. An apparatus according to claim 39, wherein the indicia is a biometric, the apparatus further comprising a database that stores a plurality of biometrics for a respective plurality of users.

45. An apparatus according to claim 44, wherein the biometric is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

1/17

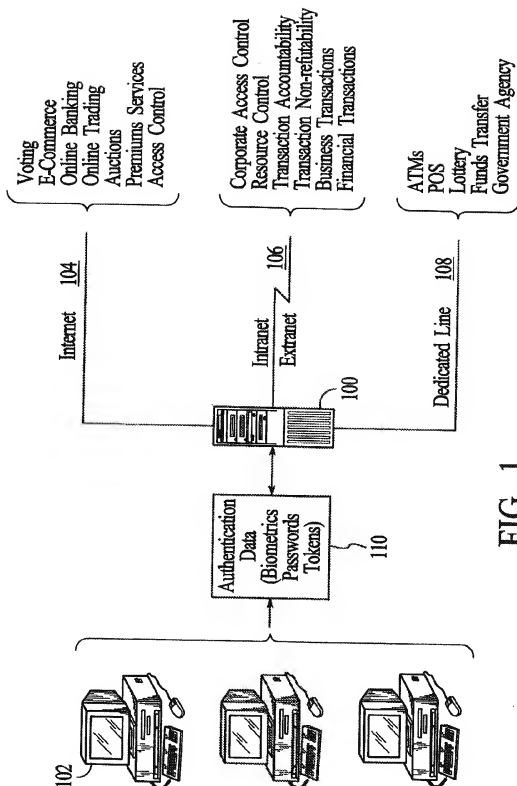
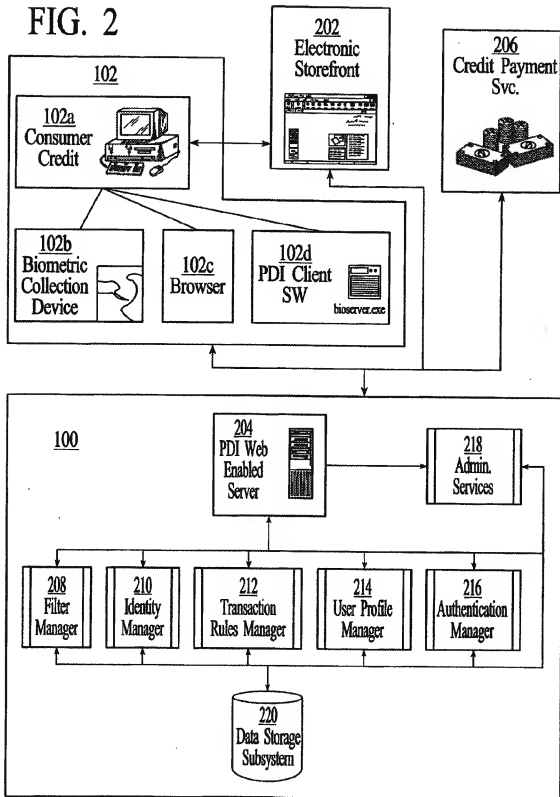


FIG. 1

SUBSTITUTE SHEET (RULE 26)

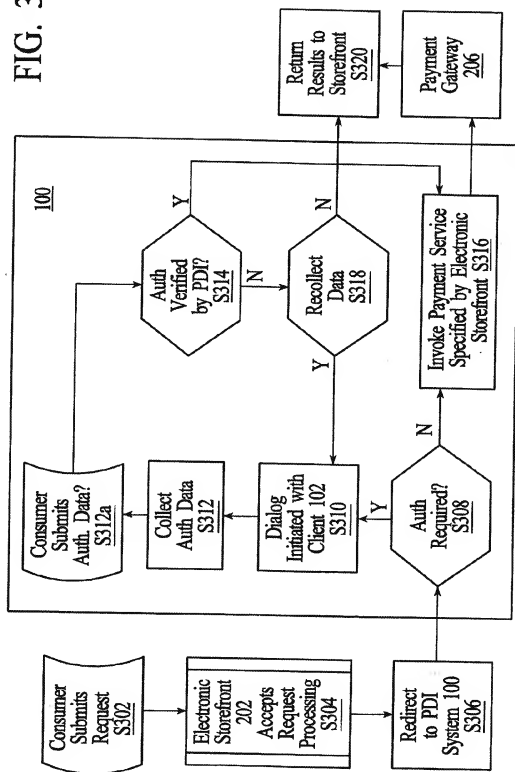
2/17

FIG. 2



3/17

FIG. 3



SUBSTITUTE SHEET (RULE 26)

4/17

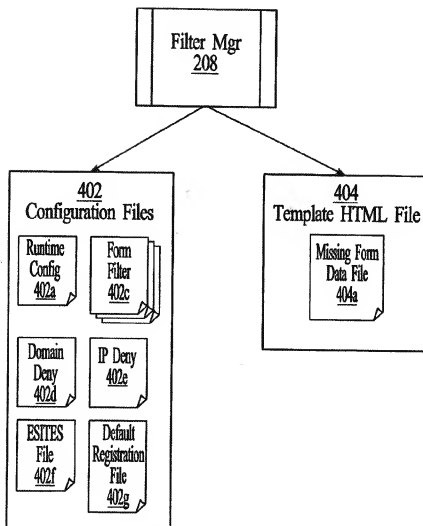


FIG. 4A

5/17

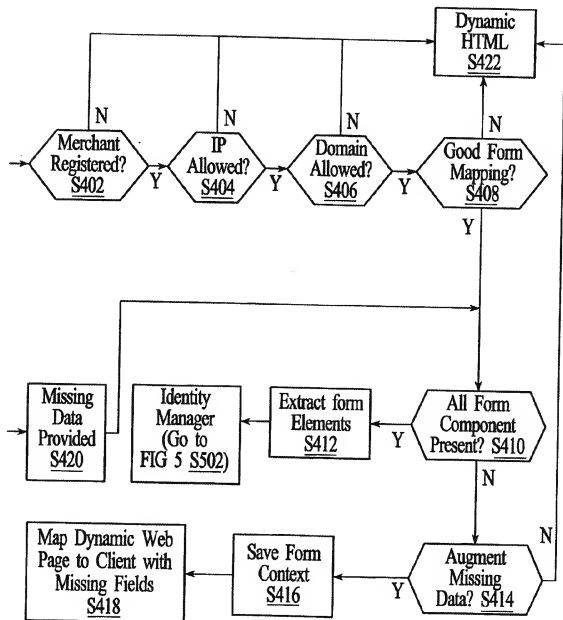


FIG. 4B

6/17

FIG. 5A

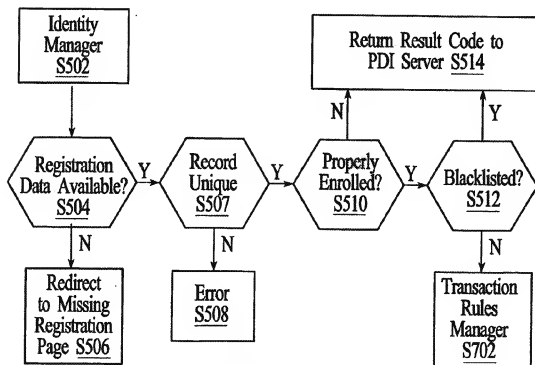
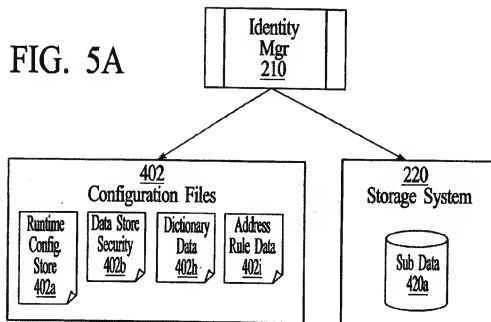


FIG. 5B

SUBSTITUTE SHEET (RULE 26)

7/17

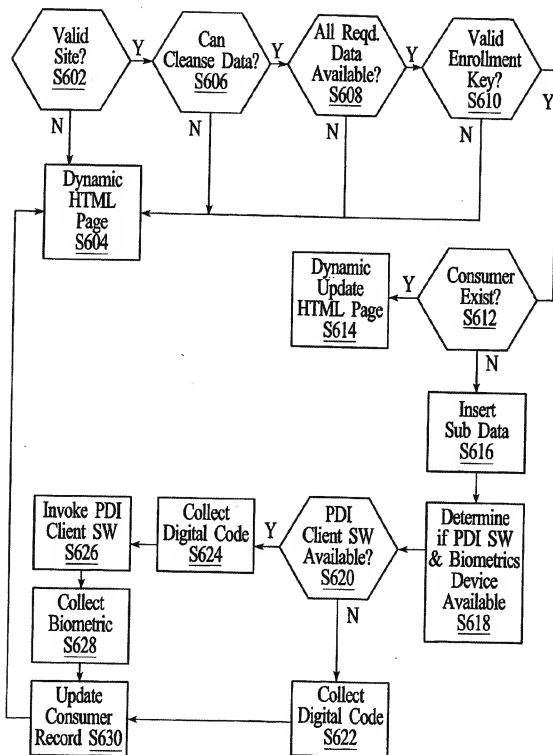


FIG. 6

8/17

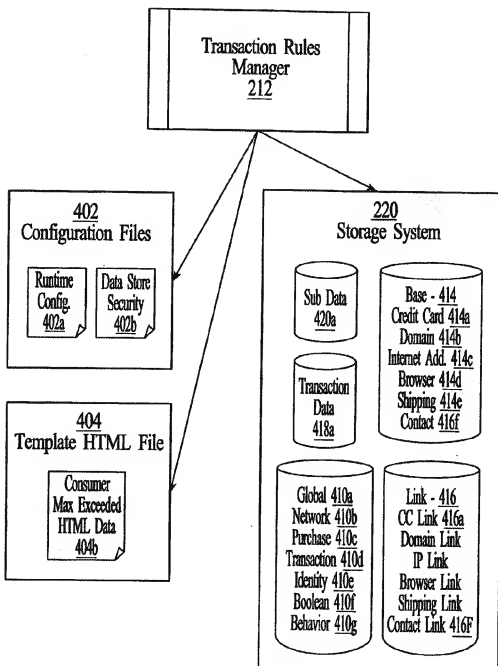


FIG. 7A

9/17

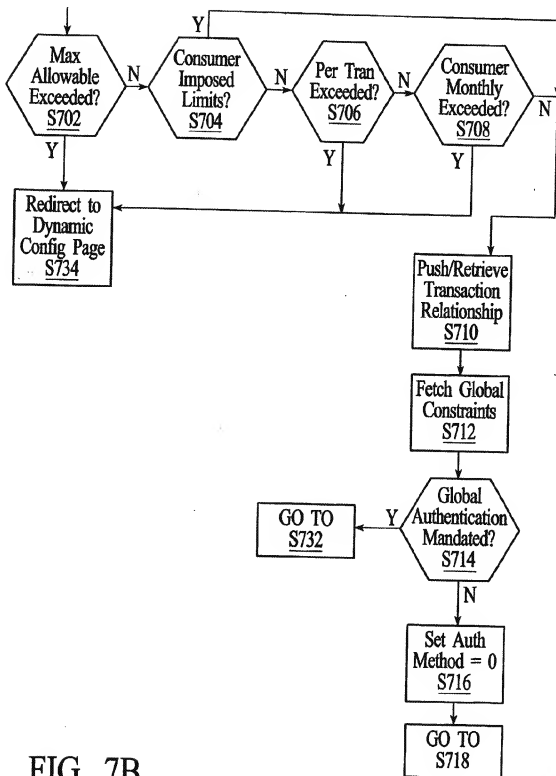


FIG. 7B

10/17

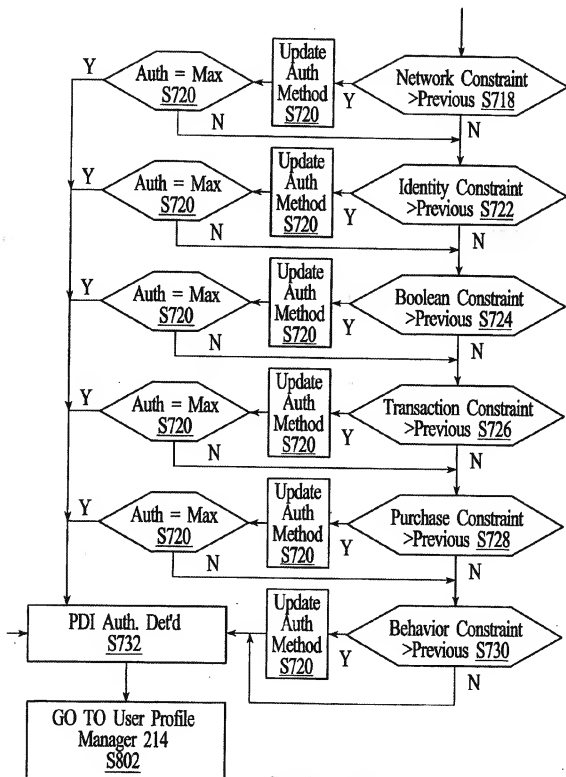


FIG. 7C

11/17

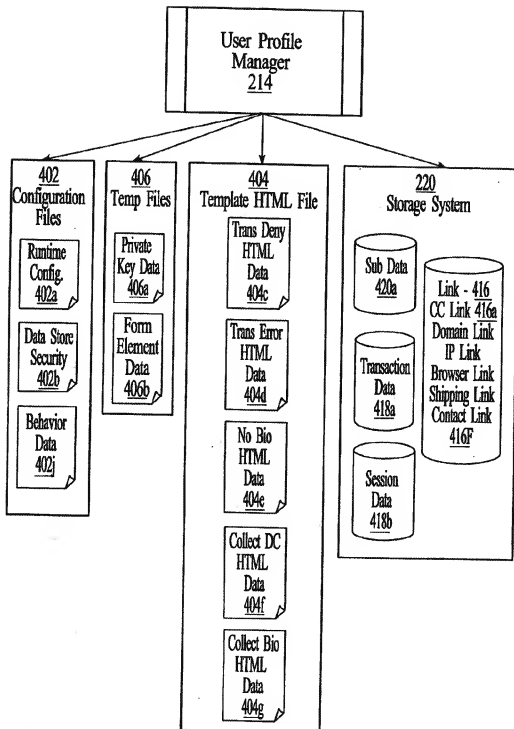


FIG. 8A

12/17

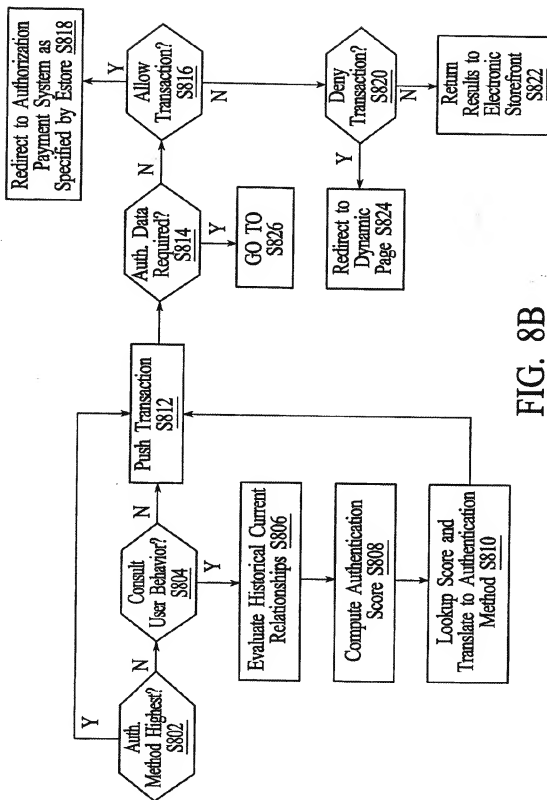
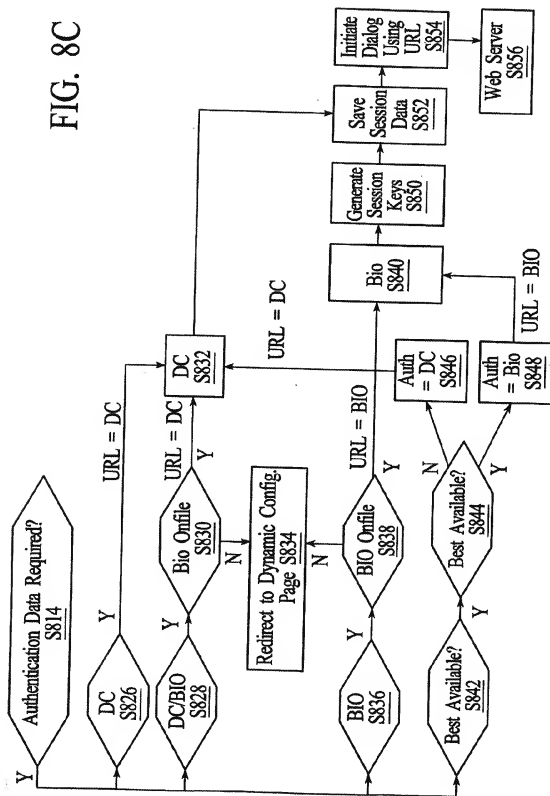


FIG. 8B

13/17

FIG. 8C



SUBSTITUTE SHEET (RULE 26)

14/17

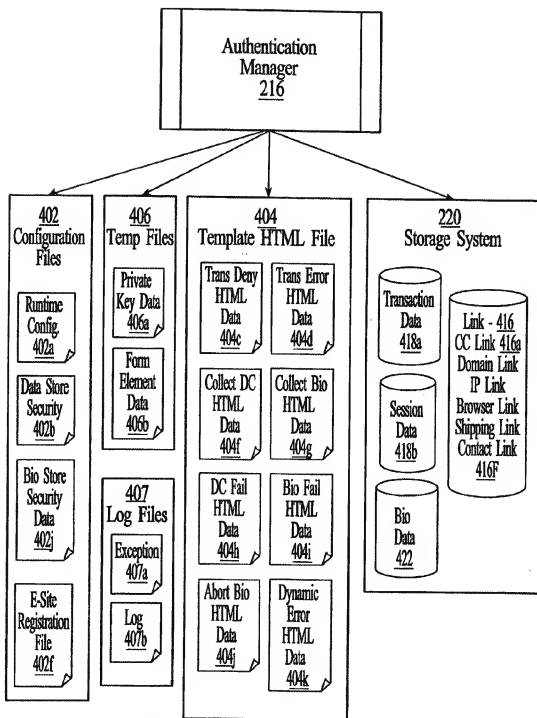


FIG. 9A

SUBSTITUTE SHEET (RULE 26)

15/17

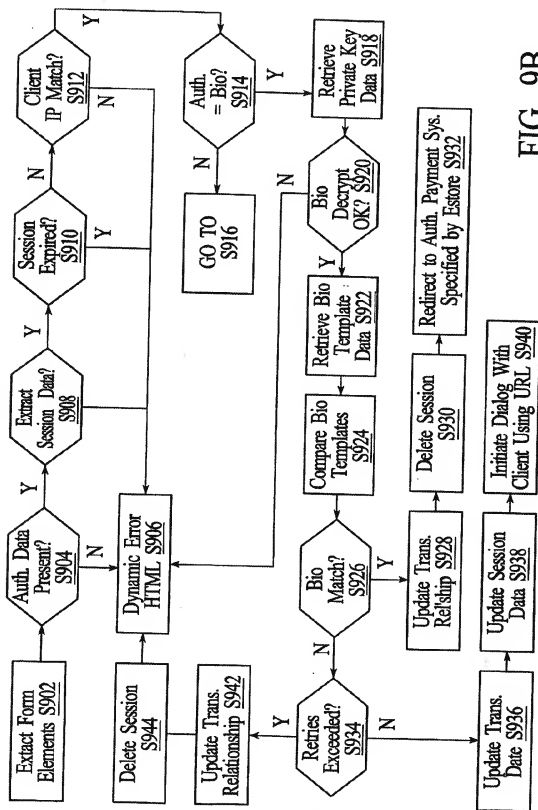


FIG. 9B

16/17

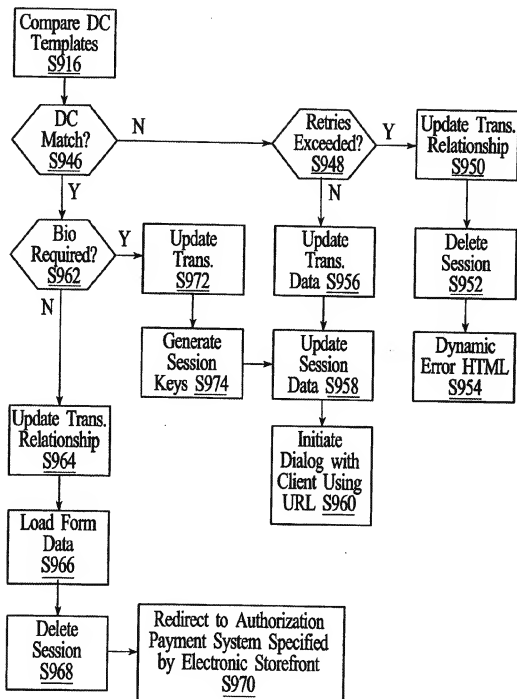


FIG. 9C

SUBSTITUTE SHEET (RULE 26)

17/17

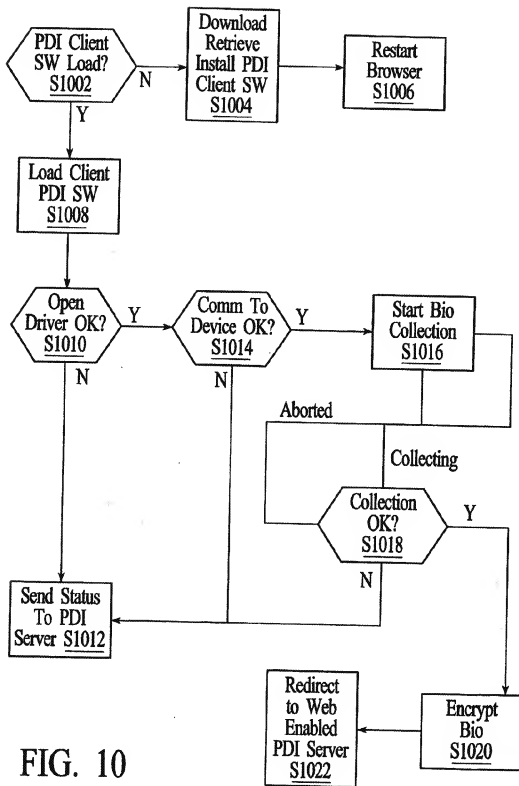


FIG. 10

SUBSTITUTE SHEET (RULE 26)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/78493 A2

- (51) International Patent Classification: Not classified
- (21) International Application Number: PCT/US01/12445
- (22) International Filing Date: 17 April 2001 (17.04.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/198,110 17 April 2000 (17.04.2000) US
09/818,084 26 March 2001 (26.03.2001) US
- (71) Applicant: VERISIGN, INC. [US/US]; 1350 Charleston Road, Mountain View, CA 94043 (US).
- (72) Inventors: GRAVES, Michael, E.; 667 Island Place, Redwood City, CA 94025 (US). FRANK, Peter, E.; 950 Redwood Shores Parkway, Redwood City, CA 94065 (US). PLAMBECK, Thane; 2341 Tasso Street, Palo Alto, CA 94301 (US). WHITEHEAD, Gregory, R.; 351 Trenton Way, Menlo Park, CA 94025 (US).
- (74) Agents: FARN, Michael, W. et al.; Fenwick & West LLP, Two Palo Alto Square, Palo Alto, CA 94306 (US).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.



WO 01/78493 A2

(54) Title: AUTHENTICATED PAYMENT

(57) Abstract: A buyer (110) wishes to use a payment instrument as part of an online commerce transaction with a seller (120) and it is desired to authenticate that the buyer (110) has authority to use the payment instrument. A separate authentication service (130) determines whether the buyer (110) has access to certain secret information without revealing the secret information to the seller (120). Access to the secret information would verify that the buyer (110) has authority to use the payment instrument. The authentication service (130) informs the seller (120) whether the buyer (110) is authorized to use the payment instrument.

AUTHENTICATED PAYMENT

5

RELATED APPLICATION

This application claims the priority benefit of U.S. Provisional Patent Application Serial Number 60/198,110, entitled "Authenticated Payment," by Greg Whitehead, Michael Graves, and Thane Plambeck, filed April 17, 2000, which subject matter is incorporated herein
10 by reference.

BACKGROUND OF THE INVENTION1. Technical Field

This invention relates to authenticating buyers in online commerce transactions and, more particularly, to having a separate authentication service authenticate the buyer.

15 2. Background Art

As a result of the increasing popularity and acceptance of the Internet and other forms of networked communications, online commerce is big business. For example, the volume of consumer purchases, business to business commerce, and stock trading and other forms of investing which occur over the Internet and/or wireless networks is steadily increasing, as are
20 other forms of online commerce. In addition, significant effort is being spent to develop alternate business models (such as auctions and group purchasing) and alternate forms of payment (such as ecash and Internet-authorized transfer of funds) in an attempt to take advantage of the unique characteristics of online commerce.

However, one of the drawbacks of online commerce is the difficulty of buyer
25 authentication. For example, consider a case in which a consumer wishes to purchase an item using a credit card. If the buyer were doing this in the real world, the buyer would be required to supply his physical credit card (perhaps with a photo on it) and would have to sign the credit card slip with a signature matching the one on the credit card. These acts accomplish two

important objectives. First, they establish with some confidence that the buyer is authorized to use the credit card. Second, they generate a record that makes it difficult for the buyer to later deny that he authorized the purchase. Both of these factors significantly reduce the risk of a fraudulent transaction.

5 In the online version of this transaction, the acts which correspond to supplying a physical credit card and signing the credit card slip either do not exist or, if they exist, are not as effective in reducing risk. For example, in many cases, the buyer is simply required to type in his credit card number and then click on a Make Purchase button. These two acts are more prone to fraud than their real world counterparts because the seller does not know if the person
10 taking these actions is actually authorized to use the credit card. In other words, it is difficult for the seller to authenticate the buyer. Furthermore, even if the true credit card owner did authorize the transaction, the increased risk of fraud means that the resulting record is not as strong since the credit card owner could allege that an impostor authorized the transaction. This extra risk of fraud in the "card not present" situation results in higher interchange rates
15 and fees for transactions processed over the Internet and other online commerce systems, and is perhaps the biggest single contributor to the cost basis for Internet commerce.

One of the reasons Internet and other online fraud has grown is that personal payment instrument information such as credit card numbers, checking account numbers, and related data has essentially become "public information" in the sense that this data is readily available.
20 For example, a consumer gives his credit card number, expiration date, etc. in an unprotected format to each online merchant in each transaction. In addition, information such as name, address, social security number, etc. is also available from sources other than the card-holder. For example, searchable, web accessible telephone directories and other types of directories can contain much of this type of information. The repeated, unprotected disclosure of payment
25 instrument information, together with the fact that much of this information is also available from other sources, increases the risk of fraudulent transactions. For example, hackers often need only to capture databases of credit card numbers and their associated name and address information in order to masquerade as the actual card-holder in many online transaction environments.

30 Conventionally, the buyer authentication problem has been addressed through the use of passwords, an approach commonly taken in Internet (web) commerce environments, where

the buyer authenticates himself typically using a simple user name and password. As described previously, passwords have inherent weaknesses when used for this purpose and current implementations further aggravate these weaknesses. For example, consumers typically must register individually with each merchant using an on-line process. As a result, the merchant has a limited opportunity to verify the consumer's registration since the timing of the on-line registration often does not permit significant verification and, even if it did, the cost would be prohibitive since each merchant would have to bear the cost of his own verification. In addition, consumers often will use the same user name and password for multiple accounts. This increases the chance that the user name and password will be compromised and, if it is compromised, increases the potential damage suffered. Furthermore, since the user name and password typically are transferred to the merchant in plaintext, unscrupulous merchants may also use this information to compromise the consumer's other accounts. As a final example, many current authentication systems target authentication of the consumer's identity (e.g., proving that the user is actually John Doe), but authenticating someone's identity is not necessarily the same as verifying that someone is authorized to use a specific payment instrument.

The Secure Electronic Transactions (or SET) protocol was one attempt to address the buyer authentication problem in order to facilitate secure payment card transactions over the Internet. In SET, digital certificates were used to create a trust chain throughout the transaction. For example, the consumer would have a digital certificate which he presented to the merchant. The merchant would have a digital certificate which he presented to the consumer. Each would verify the other's digital certificate and the underlying chain of digital certificates in order to establish trustworthiness. However, this approach imposed considerable administrative and operational complexity on consumers, merchants, and the corresponding transaction processing infrastructure. For example, both buyers and merchants required specialized technology in order to participate in the protocol and would have to upgrade the technology each time new digital certificate technology was adopted. As a result, SET was not widely adopted.

Thus, there is a need for substantial buyer authentication in online commerce transactions. There is further a need for an approach to buyer authentication which is also flexible enough to easily adapt to varying levels of security for different applications and also to the adoption of new technologies. The approach preferably also does not impose significant

burdens on or require extensive modification of the existing transaction processing infrastructure.

DISCLOSURE OF INVENTION

In accordance with the present invention, an online commerce transaction system (100) includes a buyer (110), a seller (120), and an authentication service (130). It is desired to authenticate (204) to the seller (120) that the buyer (110) is authorized to use a payment instrument as part of an online commerce transaction with the seller (120). To do this, the authentication service (130) performs the following steps, all of which occur in real-time as part of the online commerce transaction. The authentication service (130) receives (230) the request to verify that the buyer (110) is authorized to use the payment instrument. It determines (246) whether the buyer (110) has access to certain secret information without revealing the secret information to the seller (120). Access to the secret information would verify authority to use the payment instrument. Responsive to the determination of whether the buyer (110) has access to the secret information, the authentication service (130) transmits (250) to the seller (120) a response including whether the buyer (110) is authorized to use the payment instrument. In another aspect of the invention, the authentication service (130) also applies (260) profile information about the buyer (110) to the online commerce transaction and/or processes (270) or at least partially processes the payment transaction. The authentication service (130) may also store (280) a record of the use of the payment instrument and/or the transaction.

In a preferred embodiment (300), the online commerce transaction occurs over the Internet. The buyer (110) accesses the Internet via a web browser, the seller (120) operates an Internet storefront hosted by a web server, and the authentication service (130) is implemented on a web server. Furthermore, the secret information includes a private key. In other words, creating digital signatures using the private key would be proof that the signer is authorized to use the corresponding payment instrument. In this embodiment, the request (330) for authentication is triggered by the buyer's submission of a form (400), which includes an action attribute identifying the authentication service (130). The request (330) to the authentication service (130) also includes the seller's address so that the authentication service knows where to send (350) the results of its authentication process. To authenticate the seller (120), the authentication service (130) transmits (340) a challenge request to the buyer (110), requesting

that the buyer (110) use the private key to digitally sign some data. The authentication service (130) uses the buyer's response (342) to determine (346) whether the buyer (110) has access to the private key and then transmits (350) the results to the seller (120). The authentication service (130) may further request that the buyer (110) digitally sign a record of the transaction, thus creating (380) a strong record of the transaction.

The present invention is particularly advantageous because a separate authentication service (130) rather than the seller (120) is used to authenticate the buyer (110). As a result, the seller (120) does not gain access to the secret information associated with the buyer's payment instrument. This prevents the seller (120) from later reusing the secret information to authorize fraudulent transactions.

Furthermore, concentration of the authentication function in the authentication service (130) results in significant flexibility and economies of scale. Many types of secret information may be appropriate, each requiring different technology to implement. Concentrating the authentication function in the authentication service (130) allows the cost of the required technology to be shared among many sellers (120). Furthermore, if the type of secret information or the corresponding buyer authentication procedure is changed, the bulk of the changes will affect only the authentication service (130), thus permitting new authentication technologies to be easily implemented. If the authentication service (130) performs other functions, such as adding buyer profile information to the transaction, processing of the payment instrument, or making and keeping records of the transactions, additional economies of scale may be realized, since the authentication service (130) is a natural centralized point for these other functions.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other more detailed and specific objects and features of the present invention are more fully disclosed in the following specification, reference being had to the accompanying drawings, in which:

FIG. 1 is a block diagram of a system according to the present invention;

FIG. 2 is an event trace illustrating a method of operating the system of FIG. 1;

FIG. 3 is an event trace illustrating a preferred method of operating a preferred embodiment of the system of FIG. 1; and

FIGS. 4-7 are various screen shots and dialog boxes illustrating the method of FIG. 3.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

5 FIG. 1 is a block diagram of a system 100 according to the present invention. The system 100 includes a buyer 110, a seller 120 and an authentication service 130 which communicate with each other. System 100 also optionally includes a directory 140 of authentication services, which is accessible by buyer 110, and a database 150 of buyer profiles and a transaction archive 170, both of which are accessible by the authentication service 130.
10 Optional payment gateway 160 is also accessible by the authentication service 130, although in alternate embodiments, it may be the seller 120, or both the authentication service 130 and the seller 120, which accesses the payment gateway 160. The payment gateway 160 is simply the conduit through which payment transactions are forwarded to the respective financial institutions. The present invention may be used with many different types of payment
15 gateways 160 (or even no payment gateway) and is not intended to be limited to a specific type of gateway technology.

 The buyer 110 wishes to use a payment instrument as part of an online commerce transaction with the seller 120. For example, in one application, the buyer 110 is a consumer, the seller 120 is a merchant with an Internet storefront, and the consumer wishes to use his
20 credit card to purchase some product, information, or service from the merchant. As another example, the buyer 110 is an individual who connects to the seller 120 via a wireless phone or handheld personal digital assistant (PDA), the seller 120 is a bill-paying service, and the individual wishes to write "Internet checks" to pay his monthly bills. As yet another example, the buyer 110 is a corporation or individual acting on behalf of a corporation who is
25 purchasing materials or services from the corporation's supplier 120. Other examples of payment instruments include checking account routing numbers, virtual money or electronic representations of cash, pre-purchased cash value stored in electronic wallets, purchase cards, and Internet credits or coupons.

 It should be clear from these examples that many other applications are possible and
30 the terms "buyer" and "seller" are used as convenient labels but are not meant to limit these

entities. The "buyer 110" is not required to actually buy something nor is the "seller 120" required to actually sell. Similarly, the "online commerce transaction" is not limited to buy-sell transactions. Rather, the online commerce transaction could be any transaction in which the buyer 110 wishes to use a payment instrument as part of the transaction or, more generally, any transaction which would benefit from authentication of the buyer 110. As an example of an application which does not utilize a payment instrument, the "buyer" 110 might be an individual, the "seller" 120 might be an insurance company with which the buyer holds a policy, and the "transaction" might be that the buyer wishes to change his beneficiaries. The seller wishes to first authenticate the identity of the buyer before allowing access to his account.

FIG. 2 is an event trace illustrating operation 200 of system 100. The method 200 can be roughly broken down into three major parts: buyer registration 202, buyer authorization 204, and transaction recordation 206. Not all implementations will utilize all three stages 202-206 or all of the individual steps shown in FIG. 2, but they are included in this example to illustrate various aspects of the invention. In buyer registration 202, secret information which will be used in stage 204 to authenticate the buyer and payment instrument is established between the buyer 110 and the authentication service 130. Buyer registration 202 preferably occurs only once per payment instrument. Buyer authorization 204 occurs in real-time as part of the online commerce transaction. In this stage, the buyer 110 demonstrates access to the secret information to the authentication service 130. If this access is successfully demonstrated, the authentication service 130 informs the seller 120 that the buyer 110 is authorized to use the payment instrument. In the transaction recordation 206 stage, the authentication service 130 creates a record of the transaction, and this record may be subsequently used as evidence of whether a certain transaction occurred.

The use of a separate authentication service 130 has many advantages. For example, as will be more apparent from the descriptions below, the bulk of the buyer authentication process 204 is performed by authentication service 130. The authentication service 130 determines whether the buyer 110 has demonstrated access to the secret information and therefore is authorized to use the payment instrument. The buyer 110 is only minimally involved and the seller 120 is essentially not involved at all. Concentration of this function in the authentication service 130 results in significant flexibility and economies of scale. For example, different types of secret information ranging from simple PIN numbers to

sophisticated digital certificate protocols can be used to yield different levels of security for different payment instruments. Different types of secret information typically will require different infrastructure to perform the buyer authentication stage 204. Concentrating the buyer authentication stage 204 in the authentication service 130 allows the cost of this infrastructure to be shared among many sellers 120. Furthermore, if the type of secret information or the corresponding buyer authentication procedure is changed, the bulk of the changes will affect only the authentication service 130, thus permitting new authentication technologies to be easily implemented. In contrast, previous approaches, such as SET, required each seller 120 to provide much of the necessary infrastructure. This led to high costs, slow initial adoption, and difficulty in switching to new technologies, which ultimately led to the failure of SET and similar approaches.

This approach is also advantageous because the seller 120 does not gain access to the buyer 110's secret information since the seller is not involved in buyer authentication 204. This prevents the seller 120 from later reusing the buyer 110's secret information to authorize fraudulent transactions. For example, assume that the secret information is a PIN number. If the seller 120 were responsible for buyer authentication 204, the buyer 110 would disclose his PIN number to the seller 120, who would be able to use it later for fraudulent purposes. However, in the current approach, the seller 120 discloses the PIN number only to the authentication service 130 and not to the seller 120.

Furthermore, since the buyer authentication stage 204 is concentrated in the authentication service 130, additional economies of scale may be realized by having the authentication service 130 also perform other functions, as will be further discussed below. For example, the authentication service 130 might add additional information to the transaction (e.g., the buyer's shipping address), process or partially process the buyer's payment instrument and/or make and keep records of the transactions.

Referring again to FIG. 2, each of the dashed boxes 110, 120, and 130 represents one of the components in system 100. The solid boxes represent various steps in method 200. The location of a solid box within a dashed box indicates that the step is generally performed by that component. For example, step 210 is located within the dashed box for authentication service 130. This indicates that the authentication service 130 generally performs step 210. Some steps have two boxes, indicating that the steps occurs over two components. For

example, one component may send a message to another component. The steps preferably are implemented by software running on the various components within system 100, possibly assisted by hardware modules. They can also be implemented in hardware and/or firmware.

The buyer registration stage 202 preferably occurs before the actual online commerce
5 transaction. In this stage 202, the secret information is established between the buyer 110 and the authentication service 130. The information is secret in the sense that, ideally, it is known and/or accessible only by the buyer (or by the buyer 110 and the authentication service 130 in the case of a secret shared by the two). It is not generally available to the public or to the sellers 120. Furthermore, the secret information corresponds to a specific payment
10 instrument(s) and proving access to the secret information will be taken as authorization to use the payment instrument.

Different types of secret information may be used depending on the type of security required. Examples of secret information include a PIN number or password, a network-stored credential (e.g., to support roaming), a "roaming" digital signature capability, a software
15 credential such as a private key local to the buyer's machine, a hardware credential such as a hardware token or a private key carried on a smart card, a biometric credential, and information used in cryptographic challenge response protocols.

In the specific example of FIG. 2, the secret information is established as follows. The authentication service 130 receives 210 confirmation information which enables the
20 authentication service to later determine whether the buyer 110 has access to the secret information. The authentication service 130 then stores 212 this confirmation information associated with the payment instrument, for example as part of the buyer profile database 150. In one embodiment which follows this model, the buyer's secret information is a private key and the corresponding confirmation information is the corresponding public key.

In alternate embodiments, buyer registration 202 is implemented in other ways. For example, the confirmation information may not be stored at the authentication service 130. Instead, it may be stored elsewhere and retrieved by the authentication service 130 when
25 required. Alternately, rather than storing confirmation information which is different from the secret information, the authentication service 130 may simply store the secret information itself (e.g., storing passwords or hashes of passwords). As another example, buyer registration
30 itself (e.g., storing passwords or hashes of passwords). As another example, buyer registration

202 may occur offline. For example, the buyer 110 might fill out an application and send it to a bank. The bank verifies the information on the application, issues a credit card to the buyer 110, and sends the account information to the authentication service 130. The authentication service 130 creates a smart card with embedded secret information and the smart card is sent to the buyer 110, for example via the postal service. Note that in this last example, buyer registration 202 takes advantage of the credit card enrollment process. Buyer registration may also take advantage of other processes.

The secret information preferably is generated by the buyer 110 so as to minimize its disclosure to other parties. However, in alternate embodiments, it may be generated and/or shared by other parties, for example the authentication service, particularly when the risk posed by those parties is considered to be low.

In the buyer authentication stage 204, the buyer 110 wishes to use the payment instrument as part of an online commerce transaction with the seller 120. The authentication service 130 determines in real-time as part of the transaction whether the buyer 110 is authorized to do so. In the specific example of FIG. 2, this occurs as follows. The buyer 110 offers 220 to use the payment instrument. For example, the buyer 110 may offer to pay for a purchase using a credit card.

The seller 120 would like to know whether the buyer 110 is authorized to use the payment instrument, so he sends 230 a request to the authentication service 130 to verify the buyer's authority. Depending on the payment instrument, the identity of the authentication service 130 might not be immediately apparent. There may be more than one authentication service; for example, each credit card company might provide its own authentication service. One way to resolve this problem is with a directory 140 which associates authentication services with payment instruments. In this case, seller 120 accesses the directory 140 in order to determine which authentication service is the appropriate one for the payment instrument presented by the buyer 110.

The authentication service 130 determines whether the buyer 110 has access to the secret information in steps 240-246. The authentication service 130 sends 240 a "challenge request" to the buyer 110. The challenge request asks for proof that the buyer has access to the secret information. For example, if the secret information is a password, the challenge request

may ask for the password. If the secret information is a private key, the challenge request may request that the buyer 110 digitally sign something using the private key. In one embodiment, the challenge request also includes a description of the online commerce transaction and allows the buyer to decline the transaction, for example if the description does not match the buyer's expectations. Equivalently, the challenge request may instead ask for the buyer's consent to the transaction. If the buyer 110 wishes to move forward, he sends 242 his "challenge response" back to the authentication service 130.

The authentication service 130 retrieves 244 the earlier stored confirmation information for the payment instrument and uses the confirmation information and challenge response to determine whether the buyer 110 has access to the secret information. For example, in one embodiment of the password example, the authentication service 130 hashes the alleged password from the challenge response and compares this to the hash stored as the confirmation information. In one embodiment of the private key example, the authentication service 130 uses the public key stored as confirmation information to determine whether the digitally signed message in the challenge response really was digitally signed using the corresponding private key.

The authentication service 130 then transmits 250 to the seller 120 a response to the seller's original request. The response includes whether the buyer 110 is authorized to use the payment instrument. It may also include additional information, as will be described in the context of steps 260 and 270. Note that during buyer authentication 204, the secret information is not revealed to the seller 120.

Before moving on to steps 260 and 270, note that the authentication steps 240-250 illustrated in FIG. 2 are just one way of implementing the buyer authentication stage 204. Other implementations will be apparent. For example, the authentication service 130 could receive 230 the request for authentication from the buyer 110 rather than the seller 120. As another example, the authentication service 130 might not use a challenge request 240 and challenge response 242. Proof of access to the secret information might be included as part of the initial request 230 instead. In addition, as mentioned in the buyer registration phase 202, the authentication service 130 may use methods besides confirmation information (steps 244 and 246) to determine whether the buyer has access to the secret information.

Returning to FIG. 2, in some embodiments, the authentication service 130 may also apply 260 additional buyer profile information to the transaction. For example, the seller 120 might request that the buyer's shipping address be added to the transaction. The authentication service 130 would retrieve this information from the database 150 and add it to the ongoing transaction. This additional information may be added at various points during the transaction and may involve communications with either the buyer 110 or seller 120. In the shipping address example, the buyer 110 might be asked to verify the address and/or the seller 120 might use the address to calculate shipping charges, which in turn would change the dollar amount of the transaction.

Similarly, the authentication service 130 may also process 270 the payment transaction, for example via payment gateway 160. On the one extreme, the authentication service 130 might simply notify 250 the seller 120 that the buyer 110 is authorized to use the payment instrument, but the seller 120 takes all other steps required to process the payment instrument. On the other extreme, it may be the authentication service 130 which takes the steps to process the payment transaction. In an intermediate case, the authentication service 130 takes some steps and the buyer completes the others.

Both buyer profiling 260 and payment processing 270 are attractive because the authentication service 130 is a natural centralized point for these activities. As with the actual authentication steps 240-246, economies of scale may be realized by having the authentication service 130 perform these functions rather than requiring each individual seller 120 to do so.

In the transaction recordation stage 206, the authentication service 130 stores 280 a record of the transaction in the transaction archive 170. The trustworthiness of the record will depend on the specific application. As one example, the authentication service 130 may simply store plaintext descriptions of the transaction. As another example, digitally signed and timestamped records may be more appropriate. Continuing the password example from above, a digital signed record may be created by having the authentication service digitally sign the record using its own private key. In the private key example, the buyer 110 himself creates a digitally signed record of the transaction using his own private key. In both of these examples, the result is a persistent, digitally signed record of the transaction, which can be used by the buyer 110, seller 120 or other parties to resolve disputes about the transaction.

FIGS. 3-7 illustrate a preferred embodiment of system 100 and method 200. In the Internet embodiment, the online commerce transaction occurs over an HTTP-based system, specifically the Internet. The buyer 110 accesses the Internet using a conventional web browser. The seller 120 is a merchant who operates a web site storefront on the Internet, fictitious Pete's Soccer Emporium in this case. The storefront runs on a conventional web server. The authentication service 130 also interfaces to the Internet via a web server. The buyer 110 desires to purchase the Adidas Eqt. Predator Accelerator Cup from Pete's Soccer Emporium using his credit card as the payment instrument. The secret information used to secure the transaction is a private key associated with the payment instrument. For convenience, this embodiment shall be referred to as the Internet embodiment, but this is not meant to imply that this embodiment is the only one possible for the Internet.

FIG. 3 is an event trace illustrating operation of the Internet embodiment. As with method 200, method 300 can be roughly broken down into three major parts: buyer registration 302, buyer authorization 304, and transaction recordation 306. However, the steps for buyer authorization 304 and transaction recordation 306 are intertwined with each other.

In the buyer registration phase 302, the buyer 110 sets up his "account" with the authentication service 130. In this case, this means that any offline investigation is conducted (e.g., receiving confirmation from the credit card company that the buyer 110 is authorized to use the credit card). In addition, a private key-public key pair for the account is generated and the public key is stored 312 in the authentication service's database 150. In a preferred embodiment, the public key is stored in the form of a digital certificate representing that the public key is tied to the buyer's account.

In this embodiment, the account and key pair are tied to a number of payment instruments, including the specific credit card to be used. In other words, the digital certificate and key pair are for the buyer's "wallet" which contains many payment instruments, rather than for one specific payment instrument. However, other embodiments may use different schemes, such as using a different account and key pair for each payment instrument. In addition, the buyer 110 may have a number of accounts and key pairs. In this embodiment, the buyer's private keys and associated public key infrastructure (PKI) services are managed for the buyer 110 by a software agent, specifically the VeriSign Personal Trust Agent (PTA). The

PTA provides general purpose key and certificate management functionality and is designed to be easily incorporated into web applications.

The VeriSign PTA manages the buyer's PKI credentials. For example, if the buyer 110 does not have a digital certificate or key pair, the PTA takes the buyer 110 to a certificate enrollment page. If the buyer's digital certificate will soon expire, the PTA prompts the buyer 110 to renew the certificate before continuing and can take the buyer 110 to the certificate renewal page. Similarly, if the buyer's certificate has already expired, the PTA offers the option to go to the certificate renewal page to renew the expired certificate. All of this is implemented by a set of dialogs that are consistent across different browsers. Furthermore, although this specific embodiment uses browsers, the PTA also supports other devices, such as wireless phones and handheld PDAs.

The PTA and private keys may be hosted in a number of locations. In this example, a separate server (not shown) hosts the software implementing the PTA and stores the corresponding private keys. One advantage of this approach is that since the PTA and private keys are implemented as a zero-client, hosted service, no changes need be made to the buyer's browser. Another advantage is that since the buyer's browser does not require any special software, the buyer 110 potentially can access the PTA and his private keys from any standard browser. For an example of how this may be implemented, see co-pending U.S. Patent Application Serial No. 09/574,687, "Server-Assisted Regeneration of a Strong Secret from a Weak Secret," by Warwick Ford, filed May 17, 2000, which subject matter is incorporated herein by reference. If the server hosting the PTA is the same as the one hosting the authentication service 130, the two functions may be integrated to some degree. In an alternate embodiment, the PTA and/or corresponding private keys are implemented on the buyer's client. For example, the PTA may be implemented as a plug-in (e.g., ActiveX control) to the buyer's browser and the private keys stored locally on the buyer's client or in dedicated hardware (e.g., a hardware token).

Continuing the soccer example, after registering 302, the buyer 110 is shopping at Pete's and decides to buy some products. FIG. 4 is a screen shot of the buyer's browser as he is beginning the checkout process. The HTML order form 400 includes an order area 410 and also a button 420 for express, authenticated payment. The order area indicates that the total plus tax for this order is \$59.95. The buyer 110 could check out in an unauthenticated manner

using the rest of the form, filling in credit card information, billing address, etc. However, the buyer 110 wishes to use authenticated payment and instead clicks the button 420 for "AuthPay" (i.e., authenticated payment).

As a result of clicking the authenticated payment button 420, a request for authentication is sent 330 from the buyer's browser to the authentication service 130. The request includes a description of the payment transaction and also identifies the seller 120. The authentication service 130 determines whether the buyer 110 has access to the secret information (in this case, the private key for the selected account) in steps 340-346. In particular, the authentication service 130 sends 340 a challenge request to the buyer 110. The challenge request asks the buyer 110 to digitally sign some data using the private key for the selected account. The buyer 110 sends 342 his challenge response back to the authentication service 130. The authentication service 130 retrieves the earlier stored public key and uses it to determine 346 whether the buyer 110 has access to the corresponding private key. The authentication process typically is carried out between computers without the human buyer 110's active participation.

In this embodiment, the PTA is also invoked in order to allow the buyer 110 to select which of his accounts he wishes to use and later to select the specific payment instrument from within the account. More specifically, clicking button 420 causes the buyer's web browser to interact with the PTA via the dialog boxes in FIGS. 5A and 5B. In FIG. 5A, the buyer 110 specifies which account he wishes to use by filling in the User Name field 510 and then authenticates himself to the PTA by filling in the correct password 520. The PTA displays the dialog box of FIG. 5B, which includes a visual representation 530 of the account selected. The buyer 110 confirms that he wishes to use this account by clicking on the Login button 540. The private key for the account is now available for authentication and digital signature.

If the buyer 110 fails the authentication step,, the authentication service 130 takes appropriate actions. For example, it might notify the seller 120 that the buyer was not authenticated. Alternately, it may refuse to further process the transaction and return the buyer 110 to an earlier screen (e.g., the check-out screen 400).

If the buyer 110 is authenticated, the authentication service 130 applies 360 additional buyer profile information to the transaction. In this case, the authentication service 130

retrieves buyer profile information and sends this information to the browser as the form shown in FIG. 6. The information includes the different payment instruments 610 in this account and also different shipping addresses 620. This buyer profile information can be of a sensitive nature so it is preferable that the authentication service 130 authenticate the buyer 5 110 before sending the information to him. The form also reiterates information 630 about the transaction. The buyer 110 selects the payment instrument 610 and billing address 620 and submits the form by clicking the Continue button.

The buyer 110 and authentication service 130 create 380 a digitally signed record of the transaction using the form and dialog box shown in FIGS. 7A and 7B. In response to the 10 submission of the form 600, the authentication service 130 returns the form of FIG. 7A which contains a summary 710 of the transaction and requests that the buyer 110 authorize the transaction. The buyer 110 does so by clicking on the Authorize Transaction button 720. This invokes the PTA dialog box of FIG. 7B. By clicking the Sign button 730, the buyer causes the PTA to digitally sign the summary, thus creating a digitally signed record of the transaction. 15 The authentication service 130 then notifies 350 the seller 120 that the buyer is authorized to use the payment instrument and preferably also notifies the buyer that the transaction was approved.

In this embodiment, the authentication service 130 also processes 370 the payment instrument for the seller 120 via a payment gateway 160, such as the Payflow service available 20 from VeriSign.

The transmission of information between the buyer 110, seller 120 and authentication service 130 in method 300 is accomplished using conventional web techniques. For example, note that form 400 is served by the seller 120 but clicking on the authenticated payment button 420 hands off the buyer's browser from the seller 120 to the authentication service 130. 25 Similarly, once the authentication process is completed, the buyer's browser is returned from the authentication service 130 to the seller 120.

Both of these transfers are accomplished using conventional techniques, such as GET, POST, and/or redirect. For example, the transfer can be accomplished by an HTTP POST of a form containing the data to be conveyed. This is robust but sometimes results in unwanted, 30 intermediate web pages. However, an automatically triggered client script can be used to

eliminate the need to click through the intermediate pages. Another option is HTTP redirect to a URL which contains the data to be conveyed. This can eliminate intermediate pages but is currently limited in the amount of data that can be conveyed (since only HTTP GETs can be redirected). Another option is HTTP redirect to a URL which references the location of the data to be conveyed, with the data actually transferred via some other mechanism. This is more complex than the other two methods, but can eliminate intermediate pages without limiting the amount of data that can be conveyed. The data is transmitted by some other mechanism and at the destination, it is assigned an identifier and cached. The buyer 110 is then redirected with a URL containing the assigned identifier.

As a simplified example, assume for the moment that clicking the authenticated payment button 420 sends a request for authentication to the authentication service 130. In one embodiment, this is achieved by using a form 400 with the following structure:

```

15  <form method=post action="https://authpay.verisign.com/authenticate.dll">
    <input type="hidden" name="returnURL" value="https://www.seller.com/process">
    <input type="hidden" name="msg" value="PayerAuth Request goes here">
    <input type="submit" value="Auth Pay">
  </form>

```

https://authpay.verisign.com/authenticate.dll is the URL of the authentication service 130.

The **returnURL** field specifies a location at the seller 120's web site to which the buyer 110 is returned after authentication is completed. The **msg** field carries the request for authentication. Other fields may be used to support additional functionality, such as applying profile information or payment processing.

Upon completion of the payment authorization process, the buyer 110 is handed from the authentication service 130 back to the seller 120 via an HTTP POST to the **returnURL** specified in the request. The HTML form posted back to the seller 120 has the following structure:

```

30  <form method=post action="https://www.seller.com/process">
    <input type="hidden" name="transID" value="123456789">
    <input type="hidden" name="msg" value="PayerAuth Response goes here">
    <input type="submit" value="Continue">
  </form>

```

The **transID** field contains a transaction identifier that can be used by either the buyer 110 or seller 120 to refer to the transaction in the transaction archive 170. The **msg** field carries the response from the authentication service 130 to the seller 120.

Although the invention has been described in considerable detail with reference to
5 certain preferred embodiments thereof, other embodiments are possible. For example, in a
wireless (e.g. WAP-based) embodiment, some or all of the communications between buyer
110, seller 120 and authentication service 130 occur via wireless connections or via gateways
connecting the wireless infrastructure to the wired infrastructure. For example, the buyer 110
might be communicating from a WAP-enabled handheld device. Therefore, the scope of the
10 appended claims should not be limited to the description of the preferred embodiments
contained herein.

claims:

1. In an online commerce transaction system including a buyer, a seller, and an authentication service, a processor-implemented method for authenticating to the seller that the buyer is authorized to use a payment instrument as part of an online commerce transaction, the
5 method comprising:
in real-time as part of the online commerce transaction, the authentication service performing the steps of:
receiving a request to verify that the buyer is authorized to use the payment instrument;
10 determining whether the buyer has access to secret information without revealing the secret information to the seller, wherein access to the secret information verifies authority to use the payment instrument; and
responsive to the determination of whether the buyer has access to the secret information, transmitting to the seller a response including whether the
15 buyer is authorized to use the payment instrument.
2. The method of claim 1 wherein, in real-time as part of the online commerce transaction, the authentication service further performs the step of:
applying profile information about the buyer to the online commerce transaction.
3. The method of claim 1 further comprising:
20 responsive to a determination that the buyer has access to the secret information, the authentication service at least partially processing the payment instrument.
4. The method of claim 1 further comprising:
the authentication service storing a record of the use of the payment instrument.
5. The method of claim 4 wherein the record has been digitally signed by the buyer.
- 25 6. The method of claim 4 wherein the record has been digitally signed by the authentication service.
7. The method of claim 1 further comprising:
prior to the online commerce transaction, the authentication service performing the steps of:

receiving confirmation information which enables the authentication service to
determine whether the buyer has access to the secret information; and
storing the confirmation information;
wherein the step of determining whether the buyer has access to secret information
5 comprises:
retrieving the confirmation information; and
using the confirmation information to determine whether the buyer has access
to the secret information.

8. The method of claim 1 wherein the step of receiving a request to verify that the buyer
10 is authorized to use the payment instrument includes receiving the request as a result of an
offer from the buyer to use the payment instrument.

9. The method of claim 1 wherein the online commerce transaction system is an HTTP-
based web system.

10. The method of claim 9 wherein the secret information comprises a private key, and the
15 private key and a corresponding public key form a key pair for use in public-key cryptography.

11. The method of claim 10 wherein in real-time as part of the online commerce
transaction, the authentication service further performs the step of:
receiving an offer from the buyer to use the payment instrument, wherein the offer is
digitally signed using the private key.

20 12. The method of claim 9 wherein the step of receiving a request to verify that the buyer
is authorized to use the payment instrument comprises:
receiving the request as a result of the buyer submitting a form for the online
commerce transaction using a web browser, the form comprising:
an action attribute identifying the authentication service; and
25 a method attribute for transmitting the request to the authentication service as a
result of the buyer's submission of the form.

13. The method of claim 12 wherein:
the request further comprises an address for the seller; and

the step of transmitting to the seller a response comprises transmitting the response to the address included in the request.

14. The method of claim 9 wherein the step of determining whether the buyer has access to secret information comprises:

5 transmitting to the buyer a challenge request requesting proof that the buyer has access to the secret information;
receiving from the buyer a challenge response allegedly proving that the buyer has access to the secret information; and
determining on the basis of the challenge response whether the buyer has access to the
10 secret information.

15. The method of claim 14 wherein the challenge request further comprises:
a description of the online commerce transaction for which the payment instrument is to be used; and
a request for the buyer's consent to use the payment instrument for the online
15 commerce transaction.

16. The method of claim 9 wherein the step of transmitting to the seller a response including whether the buyer is authorized to use the payment instrument comprises POSTing the response to the seller.

17. A software program product for authenticating to a seller that a buyer is authorized to use a payment instrument as part of an online commerce transaction, the software program product controlling the operation of a processor by execution of the software by the processor, the software executing the steps of:

in real-time as part of the online commerce transaction:
receiving a request to verify that the buyer is authorized to use the payment
25 instrument;
determining whether the buyer has access to secret information without revealing the secret information to the seller, wherein access to the secret information verifies authority to use the payment instrument; and

responsive to the determination of whether the buyer has access to the secret information, transmitting to the seller a response including whether the buyer is authorized to use the payment instrument.

18. The software program product of claim 17 wherein, in real-time as part of the online commerce transaction, the software further performs the step of:
applying profile information about the buyer to the online commerce transaction.
19. The software program product of claim 17 wherein the software further performs the step of:
responsive to a determination that the buyer has access to the secret information, at least partially processing the payment instrument.
20. The software program product of claim 17 wherein the software further performs the step of:
storing a record of the use of the payment instrument.
21. The software program product of claim 20 wherein the software further performs the step of:
digitally signing the record.
22. The software program product of claim 17 wherein the step of determining whether the buyer has access to secret information comprises:
retrieving confirmation information; and
using the confirmation information to determine whether the buyer has access to the secret information.
23. The software program product of claim 17 wherein the software program product is adapted for execution by a web server.
24. The software program product of claim 23 wherein the secret information comprises a private key, and the private key and a corresponding public key form a key pair for use in public-key cryptography.
25. The software program product of claim 24 wherein in real-time as part of the online commerce transaction, the software further performs the step of:

receiving an offer from the buyer to use the payment instrument, wherein the offer is digitally signed using the private key.

26. The software program product of claim 23 wherein the step of receiving a request to verify that the buyer is authorized to use the payment instrument comprises:

- 5 receiving the request as a result of the buyer submitting a form for the online commerce transaction using a web browser, the form comprising:
an action attribute identifying the authentication service; and
a method attribute for transmitting the request to the authentication service as a result of the buyer's submission of the form.

10 27. The software program product of claim 26 wherein:
the request further comprises an address for the seller; and
the step of transmitting to the seller a response comprises transmitting the response to the address included in the request.

28. The software program product of claim 23 wherein the step of determining whether the
15 buyer has access to secret information comprises:

- transmitting to the buyer a challenge request requesting proof that the buyer has access to the secret information;
receiving from the buyer a challenge response allegedly proving that the buyer has access to the secret information; and
20 determining on the basis of the challenge response whether the buyer has access to the secret information.

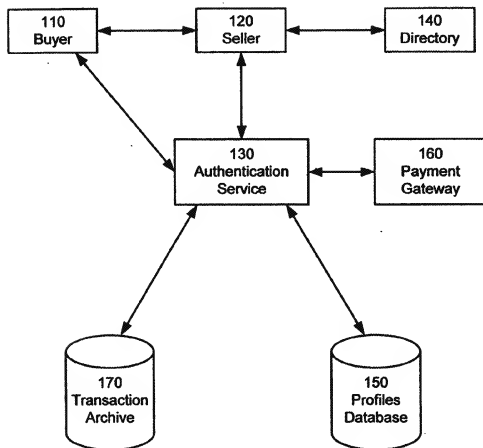
29. The software program product of claim 28 wherein the challenge request further comprises:

- a description of the online commerce transaction for which the payment instrument is
25 to be used; and
a request for the buyer's consent to use the payment instrument for the online commerce transaction.

30. The software program product of claim 23 wherein the step of transmitting to the seller a response including whether the buyer is authorized to use the payment instrument comprises
30 POSTING the response to the seller.

31. An online commerce transaction system with buyer authentication comprising:
a seller;
a buyer desiring to use a payment instrument as part of an online commerce transaction
with the seller; and
5 an authentication service communicatively coupled to the seller, for performing, in
real-time as part of the online commerce transaction, the steps of:
receiving a request to verify that the buyer is authorized to use the payment
instrument;
10 determining whether the buyer has access to secret information without
revealing the secret information to the seller, wherein access to the
secret information verifies authority to use the payment instrument; and
responsive to the determination of whether the buyer has access to the secret
information, transmitting to the seller a response including whether the
buyer is authorized to use the payment instrument.
- 15 32. The system of claim 31 wherein the authentication service is further adapted for storing
a record of use of the payment instrument.
33. The system of claim 31 wherein the authentication service is communicatively coupled
to the seller using the HTTP protocol.
- 20 34. The system of claim 31 wherein the secret information comprises a private key, and the
private key and a corresponding public key form a key pair for use in public-key cryptography.

1/9

100**Figure 1**

SUBSTITUTE SHEET (RULE 26)

2/9

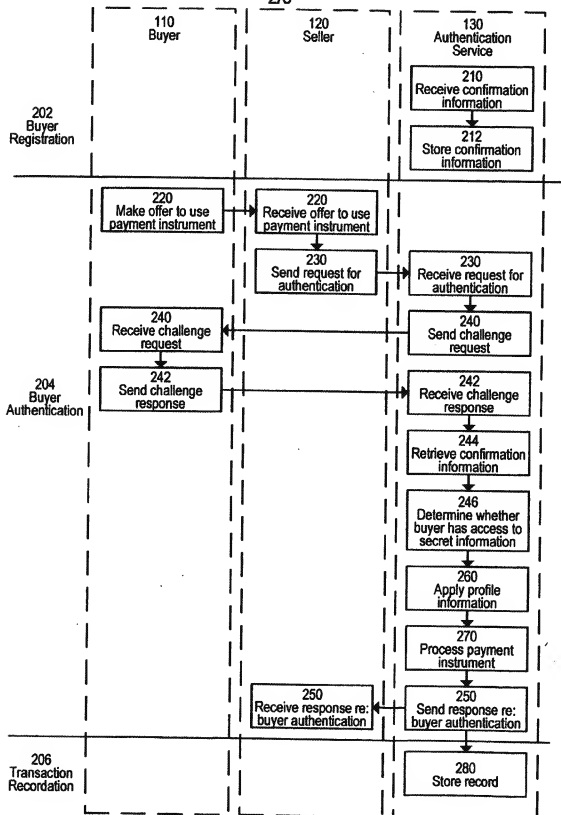


Figure 2

SUBSTITUTE SHEET (RULE 26)

3/9

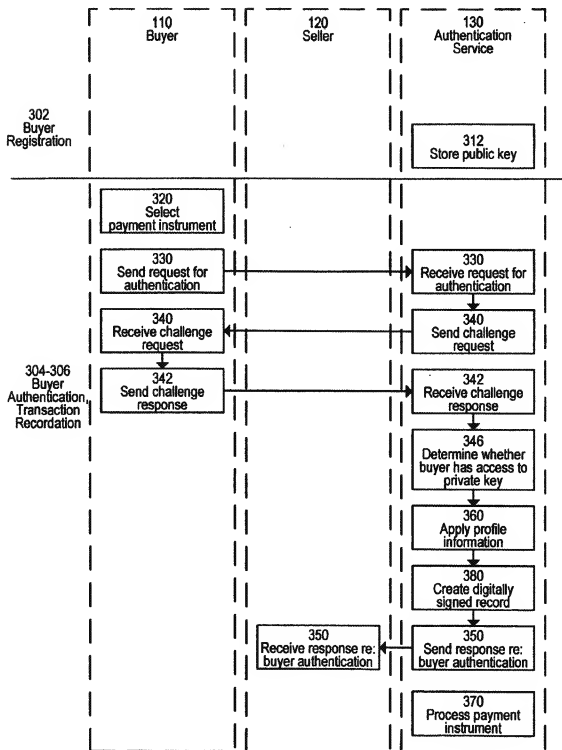


Figure 3

SUBSTITUTE SHEET (RULE 26)

400

4/9

https://pfrank*pc:8890/protected/entry.cfm?CFID=864&CFTOKEN=10680576 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Obongo

Address: https://pfrank*pc:8890/protected/entry.cfm?CFID=864&CFTOKEN=10680576 Go

Links: CNN GMSV VRSN Home Mail Google Google Scout AuthPay Demo

Pete's Soccer Emporium

Express checkout with Authpay:

Verisign
checkout

420

Order Info	
Description:	Adidas Eqt. Predator Accelerator Cup
Tax Amount:	12.30
Total Amount:	59.95
Credit Card Information	
Card Number:	
Cards Accepted - American Express - Diners Club - Discover - JCB - Mastercard - Visa	
Exp Date:	11 / 2000
Billing Information	
Name:	*
Address:	*

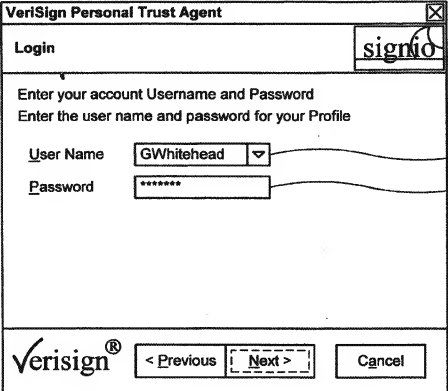
410

Local Intranet

Figure 4

SUBSTITUTE SHEET (RULE 26)

5/9



The image shows a screenshot of a software window titled "VeriSign Personal Trust Agent". The window has a standard Windows-style title bar with a close button (X) in the top right corner. Below the title bar, the word "Login" is displayed on the left, and the VeriSign logo is on the right. The main area of the window contains the text "Enter your account Username and Password" and "Enter the user name and password for your Profile". Below this text are two input fields. The first field is labeled "User Name" and contains the text "GWhitehead". The second field is labeled "Password" and contains a series of asterisks "*****". To the right of the "User Name" field, there is a small dropdown arrow. Below the input fields, there is a VeriSign logo on the left, and three buttons: "< Previous", "Next >", and "Cancel". The "Next >" button is highlighted with a dashed border. Two lines with numbers point to the input fields: line 510 points to the "User Name" field, and line 520 points to the "Password" field.

VeriSign Personal Trust Agent

Login

signio

Enter your account Username and Password
Enter the user name and password for your Profile

User Name GWhitehead 510

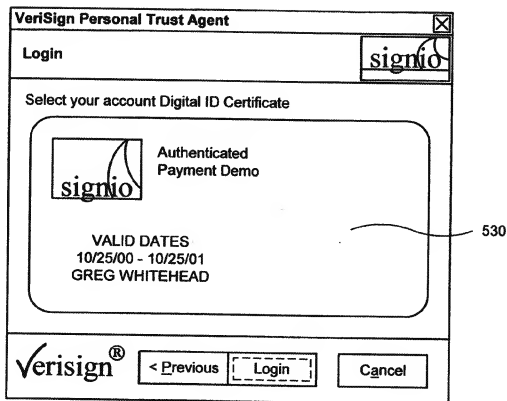
Password ***** 520

VeriSign® < Previous Next > Cancel

Figure 5A

SUBSTITUTE SHEET (RULE 26)

6/9

**Figure 5B**

SUBSTITUTE SHEET (RULE 26)

7/9

600

https://frank:9001/protected/payflowlink.cfm?CFID=101&CFTOKEN=58787548 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Obongo

Address: https://frank:9001/protected/payflowlink.cfm?CFID=101&CFTOKEN=58787548 Go

Links: CNN GMSV VRSN VRSN Day Home Mail Google Google Scout Google Search AuthPay Demo Universal Login

Pete's Soccer Emporium

Order Info	
Description:	Addidas Eqt. Predator Accelerator Cup
Tax Amount:	12.30
Total Amount:	59.95
Billing	
Billing Account:	Visa 610
Shipping	
Shipping Account:	Work 620

Continue

Local intranet

Done

Figure 6

SUBSTITUTE SHEET (RULE 26)

8/9

Confirmation - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Obongo

Address: <https://prfrank:9001/protected/authpayconfirm.cfm?CFID=101&CFTOKEN=58787548> Go

Links: [CNN](#) [GMSV](#) [VRSN](#) [VRSN Day](#) [Home Mail](#) [Google](#) [Google Scout](#) [Google Search](#) [AuthPay Demo](#) [Universal Login](#)

Pete's Soccer Emporium

Please confirm that the information below is correct.

Confirmation	
Description:	Adidas Eqt. Predator Accelerator Cup
Credit Card:	5101 XXXX XXXX 5100
Exp Date:	December 2005
Tax Amount:	12.30
Total Amount:	59.95
Bill to:	Greg Whitehead 1350 Charleston Mountain View, CA 94043 US 123-456-7890 gwhitehead@verisign.com
Ship to:	Greg Whitehead 1350 Charleston Mountain View, CA 94043 US 123-456-7890

710

720

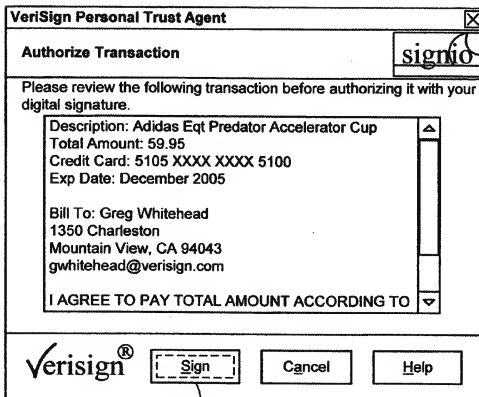
Authorize Transaction

Done Local intranet

Figure 7A

SUBSTITUTE SHEET (RULE 26)

9/9



730

Figure 7B

SUBSTITUTE SHEET (RULE 26)